FortiAuthenticator - Administration Guide

VERSION 4.2.1

FORTINET DOCUMENT LIBRARY

http://docs.fortinet.com

FORTINET VIDEO GUIDE

http://video.fortinet.com

FORTINET BLOG

https://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT

https://support.fortinet.com

http://cookbook.fortinet.com/how-to-work-with-fortinet-support/

FORTIGATE COOKBOOK

http://cookbook.fortinet.com

FORTINET TRAINING SERVICES

http://www.fortinet.com/training

FORTIGUARD CENTER

http://www.fortiguard.com

END USER LICENSE AGREEMENT

http://www.fortinet.com/doc/legal/EULA.pdf

FEEDBACK

Email: techdocs@fortinet.com

12/30/2016

FortiAuthenticator 4.2.1 - Administration Guide

23-421-400613-20161230

TABLE OF CONTENTS

Change Log

Date	Change Description
2016-12-30	Initial release.

What's new in FortiAuthenticator 4.2.1

FortiAuthenticator 4.2.1 includes a few new features designed for versatility, while maintaining ease of use.

New features include:

Allow users to change their password

Administrators can decide whether to allow local and/or remote users to change their password in the self-service portal. This feature can be configured under *Authentication* > *Self-service Portal* > *General*.

For more details, see General on page 80.

Case sensitive remote RADIUS username

Remote RADIUS usernames can be configured to being case sensitive or not. This feature can be configured under *Authentication* > *Remote Auth. Servers* > *General*.

For more details, see General on page 94.

Monitored interfaces for HA failover session pickup

FortiAuthenticator HA can be configured to monitor interfaces for automatic session pickup after failover.

If a selected service interface goes down for a configurable amount of time, the HA interface will be automatically brought down. If connectivity returns to the interface, the FortiAuthenticator will wait for a configurable delay time (e.g. 30 seconds) to ensure the port is connected correctly.

Monitored interfaces can be configured under *System* > *Administration* > *High Availability*.

For more details, see High Availability on page 35.

Certificate management enhancements

User and service certificates can be created with additional options to include OCSP URL and FQDN as a subject alternative name when generating certificates for machines.

These new options can be configured under *Certificate Management* > *End Entities* > *Users* and *Local Services*.

For more details, see End entities on page 146.

Introduction

The FortiAuthenticator device is an identity and access management solution. Identity and access management solutions are an important part of an enterprise network, providing access to protected network assets and tracking user activities to comply with security policies.

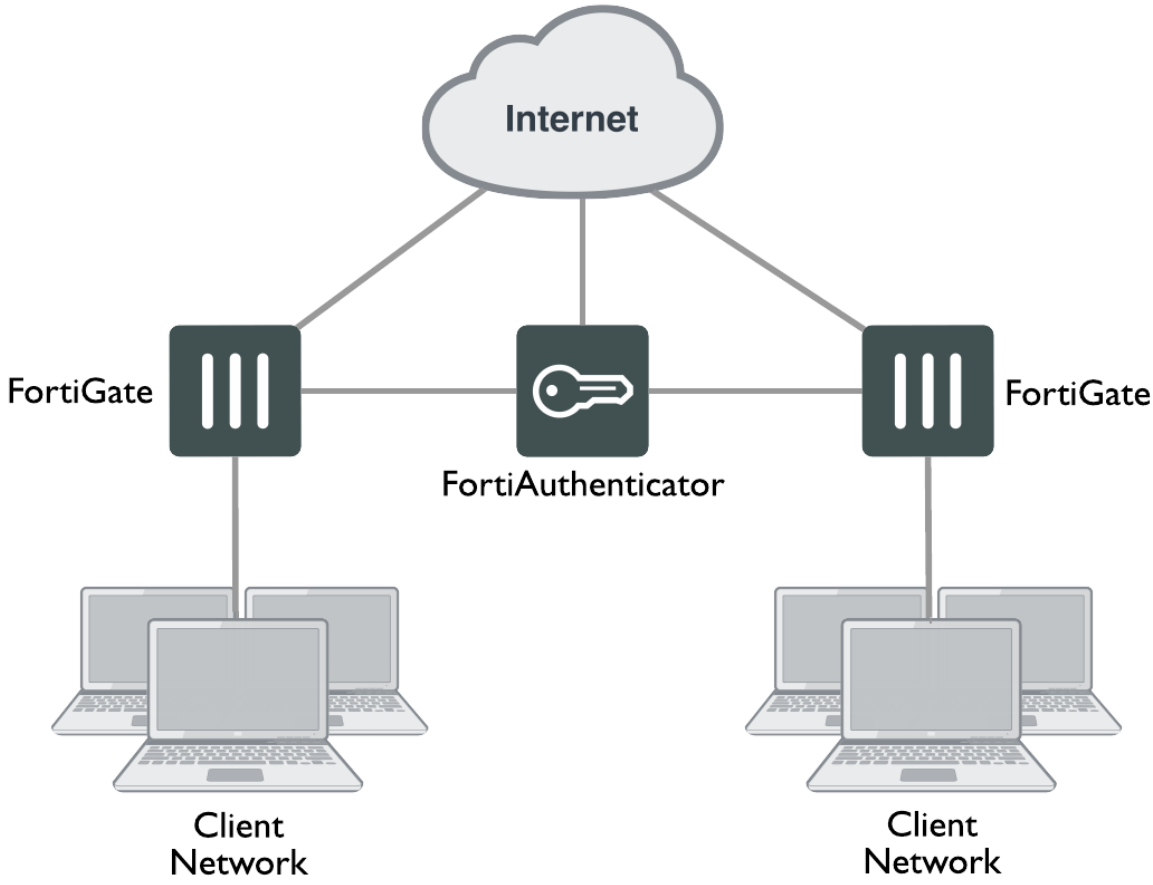
FortiAuthenticator provides user identity services to the Fortinet product range, as well as third party devices.

FortiAuthenticator delivers multiple features including:

- ***Authentication***: FortiAuthenticator includes Remote Authentication Dial In User Service (RADIUS) and Lightweight Directory Access Protocol (LDAP) server authentication methods.
- ***Two Factor Authentication***: FortiAuthenticator can act as a two-factor authentication server with support for one-time passwords using FortiToken Hardware, FortiToken Mobile, Short Message Service (SMS), or e-mail. FortiAuthenticator two-factor authentication is compatible with any system which supports RADIUS.
- ***IEEE802.1X Support***: FortiAuthenticator supports 802.1X for use in FortiGate Wireless and Wired networks.
- ***User Identification***: FortiAuthenticator can identify users through multiple data sources, including Active Directory, Desktop Client, Captive Portal Logon, RADIUS Accounting, Kerberos, and a Representational State Transfer (REST) API. It can then communicate this information to FortiGate, FortiCache, or FortiMail units for use in Identity Based Policies.
- ***Certificate Management***: FortiAuthenticator can create and sign digital certificates for use, for example, in FortiGate VPNs and with the FortiToken 300 USB Certificate Store.
- ***Integration***: FortiAuthenticator can integrate with third party RADIUS and LDAP authentication systems, allowing you to reuse existing information sources. The REST API can also be used to integrate with external provisioning systems.

FortiAuthenticator is a critical system, and should be isolated on a network interface that is separated from other hosts to facilitate server-related firewall protection. Be sure to take steps to prevent unauthorized access to the FortiAuthenticator.

FortiAuthenticator on a multiple FortiGate unit network



The FortiAuthenticator series of identity and access management appliances complement the FortiToken range of two-factor authentication tokens for secure remote access. FortiAuthenticator allows you to extend the support for FortiTokens across your enterprise by enabling authentication with multiple FortiGate appliances and third party devices. FortiAuthenticator and FortiToken deliver cost effective, scalable secure authentication to your entire network infrastructure.

The FortiAuthenticator device provides an easy-to-configure remote authentication option for FortiGate users. Additionally, it can replace the Fortinet Single Sign-On (FSSO) Agent on a Windows Active Directory (AD) network.

For more information about FortiTokens, see the FortiToken information page on the Fortinet web site.

This chapter contains the following topics:

Before you begin

Before you begin using this guide, please ensure that:

- You have administrative access to the GUI and/or CLI.

  For details of how to accomplish this, see the QuickStart Guide provided with your product, or online at http://docs.fortinet.com/fortiauthenticator/hardware.
- The FortiAuthenticator unit is integrated into your network.
- The operation mode has been configured.
- The system time, DNS settings, administrator password, and network interfaces have been configured.

Network Time Protocol (NTP) is critical for the time to be accurate and stable for the Time-based One-time Password (TOTP) method used in two-factor authentication to function correctly. See Configuring the system time, time zone, and date on page 1.

- Any third party software or servers have been configured using their documentation.

While using the instructions in this guide, note that administrators are assumed to have all permissions, unless otherwise specified. Some restrictions will apply to administrators with limited permissions.

How this guide is organized

This FortiAuthenticator Administration Guide contains the following sections:

- Setup describes initial setup for standalone and HA cluster FortiAuthenticator configurations.
- System describes the options available in the system menu tree, including: network configuration, administration settings, and messaging settings.
- Authentication describes how to configure built-in and remote authentication servers and manage users and user groups.
- Port-based Network Access Control describes how to configure the FortiAuthenticator unit for IEEE 802.1X Extensible Authentication Protocol (EAP) authentication methods, Bring Your Own Device (BYOD), and MAC-based device authentication.
- Fortinet Single Sign-On describes how to use the FortiAuthenticator unit in a Single Sign On (SSO) environment.
- RADIUS Single Sign-On describes how to use the FortiAuthenticator unit RADIUS accounting proxy.
- Monitoring describes how to monitor SSO and authentication information.
- Certificate Management describes how to manage X.509 certificates and how to set up the FortiAuthenticator unit to act as an Certificate Authority (CA).
- Logging describes how to view the logs on your FortiAuthenticator unit.
- Troubleshooting provides suggestions to resolve common problems.

Registering your Fortinet product

Before you begin configuring and customizing features, take a moment to register your Fortinet product at the Fortinet Technical Support web site at https://support.fortinet.com. Many Fortinet customer services such as firmware updates, technical support, FortiGuard Antivirus, and other FortiGuard services require product registration.

Setup

For information about installing the FortiAuthenticator unit and accessing the CLI or GUI, refer to the Quick Start Guide provided with your unit.

This chapter provides basic setup information for getting started with your FortiAuthenticator device. For more detailed information about specific system options, see System on page 1.

The following topics are included in this section:

Initial setup

The following section provides information about setting up the Virtual Machine (VM) version of the product.

FortiAuthenticator VM setup

Before using FortiAuthenticator-VM, you need to install the VMware application to host the FortiAuthenticator-VM device. The installation instructions for FortiAuthenticator-VM assume you are familiar with VMware products and terminology.

System requirements

For information on the FortiAuthenticator-VM system requirements, please see the product datasheet available at http://www.fortinet.com/products/fortiauthenticator.

FortiAuthenticator-VM has kernel support for more than 4GB of RAM in VM images. However, this support also depends on the VM player version. For more information, see: http://kb.vmware.com/selfservice/microsites/search.do?language=en_US&cmd=displayKC&externalId=1014006
The default *Hardware Version* is 4 to support the widest base of VM players. However you can modify the VM Hardware Version by editing the following line in the FortiAuthenticator-VM.vmx file:

```
virtualHW.version = "4"
```

FortiAuthenticator-VM image installation and initial setup

The following procedure describes setup on VMware Fusion.

To set up the FortiAuthenticator VM image:

1. Download the VM image ZIP file to the local computer where VMware is installed.
2. Extract the files from the zip file into a folder.
3. In your VMware software, go to *File* > *Open*.
4. Navigate to the expanded VM image folder, select the *FortiAuthenticator-VM.vmx* file, and select *Open*.
   VMware will install and start FortiAuthenticator-VM. This process can take a minute or two to complete.
5. At the FortiAuthenticator login prompt, enter `admin` and press *Enter*.
6. At the password prompt, press *Enter*. By default, there is no password.
7. At the CLI prompt enter the following commands:
   ```
   set port1-ip 192.168.1.99/24
   set default-gw 192.168.1.2
   ```
   Substitute your own desired FortiAuthenticator IP address and default gateway.

You can now connect to the GUI at the IP address you set for port 1.

Suspending the FortiAuthenticator-VM can have unintended consequences. Fortinet recommends that you do not use the suspend feature of VMware. Instead, shut down the virtual FortiAuthenticator system using the GUI or CLI, and then shut down the virtual machine using the VMware console.

Administrative access

Administrative access is enabled by default on port 1. Using the GUI, you can enable administrative access on other ports if necessary.

To add administrative access to an interface:

1. Go to *System* > *Network* > *Interfaces* and select the interface you need to add administrative access to. See Interfaces on page 1 for more information.
2. In *Admin access*, select the types of access to allow.
3. Select *OK*.

GUI access

To use the GUI, point your browser to the IP address of port 1 (192.168.1.99 by default). For example, enter the following in the URL box:

```
https://192.168.1.99
```

Enter `admin` as the *User Name* and leave the *Password* field blank.

HTTP access is not enabled by default. To enable access, use the `set ha-mgmt-access` command in the CLI (see CLI commands on page 1), or enable HTTP access on the interface in the GUI (see Interfaces on page 1).

For security reasons, the host or domain names that the GUI responds to are restricted. The list of trusted hosts is automatically generated from the following:

- Configured hostname
- Configured DNS domain name
- Network interface IP addresses that have HTTP or HTTPS enabled
- HA management IP addresses

Additional IP addresses and host or domain names that the GUI responded to can be defined in the *GUI Access* settings. See GUI access on page 1 for more information.

Telnet

CLI access is available using telnet to the port1 interface IP address (192.168.1.99 by default). Use the telnet -K option so that telnet does not attempt to log on using your user ID. For example:

```
$ telnet -K 192.168.1.99
```

At the FortiAuthenticator login prompt, enter `admin`. When prompted for password press `Enter`. By default there is no password. When you are finished, use the `exit` command to end the telnet session.

CLI access using Telnet is not enabled by default. To enable access, use the `set ha-mgmt-access` command in the CLI (see CLI commands on page 1), or enable Telnet access on the interface in the GUI (see Interfaces on page 1)

SSH

SSH provides secure access to the CLI. Connect to the port1 interface IP address (192.168.1.99 by default). Specify the user name `admin` or SSH will attempt to log on with your user name. For example:

```
$ ssh admin@192.168.1.99
```

At the password prompt press `Enter`. By default there is no password. When you are finished, use the `exit` command to end the session.

Note that, after three failed login attempts, the interface/connection will reset, and that SSH timeout is set to 60 seconds following an incomplete login or broken session.

Adding a FortiAuthenticator unit to your network

Before setting up the FortiAuthenticator unit, there are some requirements for your network:

- You must have security policies that allow traffic between the client network and the subnet of the FortiAuthenticator,
- You must ensure that the following ports are open in the security policies between the FortiAuthenticator and authentication clients, in addition to management protocols such as HTTP, HTTPS, telnet, SSH, ping, and other protocols you may choose to allow:
  - UDP/161 (SNMP)
  - UDP/1812 (RADIUS Auth)
  - UDP/1813 (RADIUS Accounting)
  - TCP/389 (LDAP)
  - TCP/636 (LDAPS)
  - TCP/8000 (FortiGate FSSO)
  - TCP/2560 (OCSP)

- TCP/8001 (FortiClient Single Sign-On Mobility Agent FSSO)
- TCP/8002 (DC/TS Agent FSSO)
- TCP/8003 (Hierarchical FSSO)

To setup FortiAuthenticator on your network:

1. Log in to the GUI with the username `admin` and no password.
2. Go to *System* > *Network* > *DNS*. Enter your internal network primary and secondary name server IP addresses. This is essential for successful FSSO operation. See DNS on page 1 for more information.
3. Go to *System* > *Network* > *Static Routing* and create a default route (IP/Mask 0.0.0.0/0) to your network gateway on the interface that connects to the gateway. See Static routing on page 1 for more information.
4. Go to System > *Dashboard* > *Status*.
5. In the *System Information* widget select *Change* in the *System Time* field, then select your time zone from the list.
6. Either enable the NTP or manually enter the date and time. See Configuring the system time, time zone, and date on page 1 for more information.

   Enter a new time and date by either typing it manually, selecting *Today* or *Now*, or select the calendar or clock icons for a more visual method of setting the date and time.

If you will be using FortiToken devices, Fortinet strongly recommends using NTP. FortiToken Time based authentication tokens are dependent on an accurate system clock.

7. Select *OK*.
8. If the FortiAuthenticator is connected to additional subnets, configure additional FortiAuthenticator interfaces as required. See Interfaces on page 1 for more information.

Maintenance

System maintenance tasks include:

- Backing up the configuration
- Upgrading the firmware
- Licensing

Backing up the configuration

You can back up the configuration of the FortiAuthenticator unit to your local computer. See Backing up and restoring the configuration on page 1 for more information.

Automatic system configuration backup can also be configured. See Automatic backup on page 1 for information.

Upgrading the firmware

Periodically, Fortinet issues firmware upgrades that fix known issues, add new features and functionality, and generally improve your FortiAuthenticator experience. See Firmware on page 1 for more information.

Before proceeding to upgrade your system, Fortinet recommends you back up your configuration. Please follow the procedure detailed in Backing up and restoring the configuration on page 1.

To upgrade the firmware, you must first register your FortiAuthenticator with Fortinet. See Registering your Fortinet product on page 1 for more information.

To upgrade FortiAuthenticator firmware:

1. Download the latest firmware to your local computer from the Fortinet Technical Support web site, https://support.fortinet.com.
2. Go to *System* > *Administration* > *Firmware*.
3. Select *Browse...*, and locate the firmware image on your local computer.
4. Select *OK*.

When you select *OK*, the firmware image will upload from your local computer to the FortiAuthenticator device, which will then reboot. You will experience a short period of time during this reboot when the FortiAuthenticator device is offline and unavailable for authentication.

Licensing

FortiAuthenticator-VM works in evaluation mode until it is licensed. The license is valid only if one of the FortiAuthenticator interfaces is set to the IP address specified in the license. See Licensing on page 1 for more information.

To license FortiAuthenticator:

1. Go to *System* > *Administration* > *Licensing*.
2. Select *Browse...* and locate on your local computer the license file you received from Fortinet.
3. Select *OK*.

CLI commands

The FortiAuthenticator has CLI commands that are accessed using SSH or Telnet. Their purpose is to initially configure the unit, perform a factory reset, or reset the values if the GUI is not accessible.

Command	Description
`help`	Display list of valid CLI commands. You can also enter `?` for help.
`exit`	Terminate the CLI session.
`show`	Display bootstrap configuration.

Command	Description
`set port1-ip <IP/netmask>`	Enter the IPv4 address and netmask for the port1 interface. Netmask is expected in the /xx format, for example `192.168.0.1/24`. Once this port is configured, you can use the GUI to configure the remaining ports.
`set default-gw <IP>`	Enter the IPv4 address of the default gateway for this interface. This is the default route for this interface.
`set date <YYYY-MM-DD>`	Enter the current date. Valid format is four digit year, two digit month, and two digit day. For example: `set date 2014-08-12` sets the date to August 12th, 2014.
`set time <HH:MM:SS>`	Enter the current time. Valid format is two digits each for hours, minutes, and seconds. 24-hour clock is used. For example 15:10:00 is 3:10pm.
`set tz <timezone_index>`	Enter the current time zone using the time zone index. To see a list of index numbers and their corresponding time zones, enter `set tz ?`.
`set ha-mode {enable | disable}`	Enable or disable (default) HA mode.
`set ha-port <interface>`	Select a network interface to use for communication between the two cluster members. This interface must not already have an IP address assigned and it cannot be used for authentication services. Both units must use the same interface for HA communication.
`set ha-priority {high | low}`	Set to `Low` on one unit and `High` on the other. Normally, the unit with High priority is the master unit.
`set ha-password <password>`	Set the HA password.
`set ha-mgmt-ip <IP/netmask>`	Enter the IP address, with netmask, that this unit uses for HA related communication with the other FortiAuthenticator unit. Format: 1.2.3.4/24. The two units must have different addresses. Usually, you should assign addresses on the same private subnet.
`set ha-mgmt-access {ssh | https | http | telnet}`	Select the types of administrative access to allow.
`set ha-dbg-level <level>`	Enter the level for HA service debug logs. Range: -4 (fatal) to 4 (debug high). Default: -2 (warn).

Command	Description
`unset <setting>`	Restore default value. For each `set` command listed above, there is an `unset` command, for example `unset port1-ip`.
`raid-add-disk <slot>`	Add a disk to a degraded RAID array.
`ha-rebuild`	Rebuild the configuration database from scratch using the HA peer's configuration.
`restore-admin`	Restore factory reset's admin access settings to the port1 network interface.
`reboot`	Perform a hard restart of the FortiAuthenticator unit. All sessions will be terminated. The unit will go offline and there will be a delay while it restarts.
`factory-reset`	Enter this command to reset the FortiAuthenticator settings to factory default settings. This includes clearing the user database. This procedure deletes all changes that you have made to the FortiAuthenticator configuration and reverts the system to its original configuration, including resetting interface addresses.
`shutdown`	Turn off the FortiAuthenticator.
`status`	Display basic system status information including firmware version, build number, serial number of the unit, and system time.
`hardware-info`	Display general hardware status information.
`disk-attributes`	Display system disk attributes.
`disk-errors`	Display any system disk errors.
`disk-health`	Display disk health information.
`disk-info`	Display disk hardware status information.
`raid-hwinfo`	Display RAID hardware status information.
`nslookup`	Basic tool for DNS debugging.
`dig`	Advanced DNS debugging.
`ping`	Test network connectivity to another network host.
`tcpdump`	Examine local network traffic.
`tcpdumpfile`	Same as `tcpdump`, but the output is written to a downloadable file that can be downloaded in the GUI.
`traceroute`	Examine the route taken to another network host.

Troubleshooting

Troubleshooting includes useful tips and commands to help deal with issues that may occur. For additional help, contact customer support. See Troubleshooting on page 1 for more information.

If you have issues when attempting authentication on a FortiGate unit using the FortiAuthenticator, there are some FortiAuthenticator and FortiGate settings to check.

In addition to these settings you can use log entries, monitors, and debugging information to determine more knowledge about your authentication problems. For help with FortiAuthenticator logging, see Logging on page 1. For help with FortiGate troubleshooting, see the FortiOS Handbook Troubleshooting and User Authentication guide chapters.

FortiAuthenticator settings

When checking FortiAuthenticator settings, you should ensure that:

- there is an authentication client entry for the FortiGate unit (see RADIUS service on page 1),
- the user trying to authenticate has a valid active account that is not disabled, and that the username and password are spelled correctly,
- the user account allows RADIUS authentication if RADIUS is enabled on the FortiGate unit,
- the FortiGate unit can communicate with the FortiAuthenticator unit, on the required ports:

  RADIUS Authentication: UDP/1812

  LDAP: TCP/389

- the user account exists
  - as a local user on the FortiAuthenticator (if using RADIUS authentication),
  - in the local LDAP directory (if using local LDAP authentication),
  - in the remote LDAP directory (if using RADIUS authentication with remote LDAP password validation),
- the user is a member in the expected user groups and these user groups are allowed to communicate on the authentication client (the FortiGate unit, for example),
- If authentication fails with the log error *bad password*, try resetting the password. If this fails, verify that the pre-shared secret is identical on both the FortiAuthenticator unit and the authentication client.

If FortiToken authentication is failing, try the following:

- Verify that the token is correctly synchronized.
- Remove the token from the user authentication configuration and verify authentication works when the token is not present.
- Attempt to log into the FortiAuthenticator with the user credentials.

These steps enable the administrator to identify whether the problem is with the FortiGate unit, the credentials or the FortiToken.

FortiGate settings

When checking FortiGate authentication settings, you should ensure that:

- the user has membership in the required user groups and identity-based security policies,
- there is a valid entry for the FortiAuthenticator device as a remote RADIUS or LDAP server,
- the user is configured either explicitly or as a wildcard user.

System

The *System* tab enables you to manage and configure the basic system options for the FortiAuthenticator unit. This includes the basic network settings to connect the device to the corporate network, the configuration of administrators and their access privileges, managing and updating firmware for the device, and managing messaging servers and services.

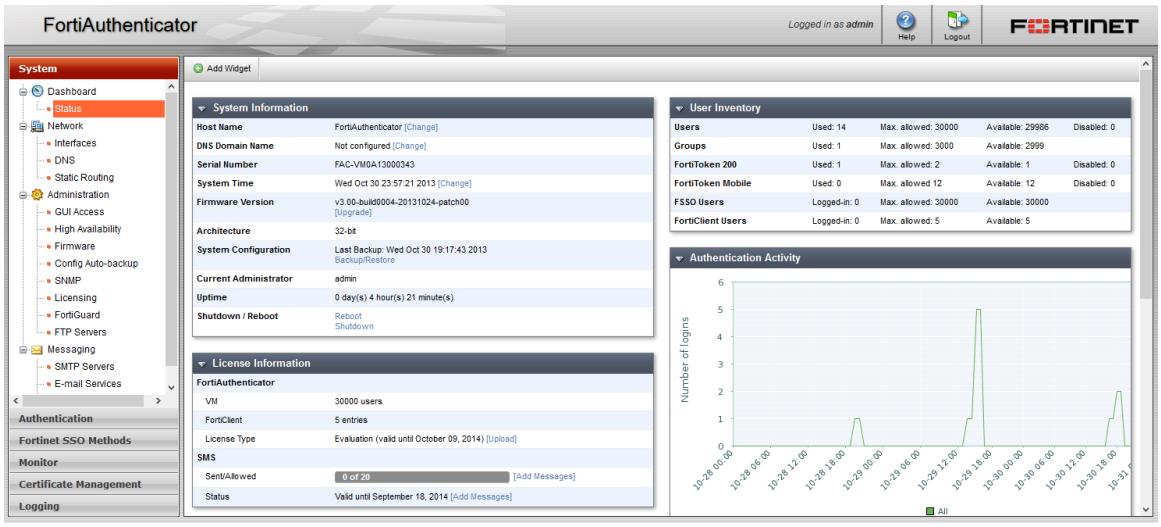
The *System* tab provides access to the following menus and sub-menus:

Dashboard	Select this menu to monitor, and troubleshoot your FortiAuthenticator device. Dashboard widgets include: • System Information • System Resources • Authentication Activity • User Inventory • HA Status • License Information • Disk Monitor • Top User Lockouts
Network	Select this menu to configure your FortiAuthenticator interfaces and network settings. • Interfaces • DNS • Static Routing • Packet Capture
Administration	Select this menu to configure administrative settings for the FortiAuthenticator device. • System Access • High Availability • Firmware Upgrade • Config Auto-backup • SNMP • Licensing • FortiGuard • FTP Servers • Admin Profiles
Messaging	Select this menu to configure messaging servers and services for the FortiAuthenticator device. • SMTP Servers • E-mail Services • SMS Gateways

Dashboard

When you select the *System* tab, it automatically opens at the *System* > *Dashboard* page.

The *Dashboard* page displays widgets that provide performance and status information and enable you to configure some basic system settings. These widgets appear on a single dashboard.



The following widgets are available:

System Information	Displays basic information about the FortiAuthenticator system including host name, DNS domain name, serial number, system time, firmware version, architecture, system configuration, current administrator, and up time. From this widget you can manually update the FortiAuthenticator firmware to a different release. For more information, see System Information widget on page 24.
System Resources	Displays the usage status of the CPU and memory. For more information, see System Resources widget on page 29.
Authentication Activity	Displays a customizable graph of the number of logins to the device. For more information, see Authentication Activity widget on page 29.
User Inventory	Displays the numbers of users, groups, FortiTokens, FSSO users, and FortiClient users currently used or logged in, as well as the maximum allowed number, the number still available, and the number that are disabled. For more information, see User Inventory widget on page 29.
HA Status	Displays whether or not HA is enabled.
License Information	Displays the device's license information, as well as SMS information. For more information, see License Information widget on page 29.

Disk Monitor	Displays if RAID is enabled, and the current disk usage in GB.
Top User Lockouts	Displays the top user lockouts. For more information, see Top User Lockouts widget on page 29.

Customizing the dashboard

The FortiAuthenticator system settings dashboard is customizable. You can select which widgets to display, where they are located on the page, and whether they are minimized or maximized.

To move a widget

Position your mouse cursor on the widget's title bar, then click and drag the widget to its new location.

To add a widget

In the dashboard toolbar, select *Add Widget*, then select the name of widget that you want to show. Multiple widgets of the same type can be added. To hide a widget, in its title bar, select the *Close* icon.

To see the available options for a widget

Position your mouse cursor over the icons in the widget's title bar. Options include show/hide the widget, edit the widget, refresh the widget content, and close the widget.

The following table lists the widget options.

Show/Hide arrow	Display or minimize the widget.
Widget Title	The name of the widget.
Edit	Select to change settings for the widget. This option appears only in certain widgets.
Refresh	Select to update the displayed information.
Close	Select to remove the widget from the dashboard. You will be prompted to confirm the action. To add the widget, select *Widget* in the toolbar and then select the name of the widget you want to show.

To change the widget title

Widget titles can be customized by selecting the edit button in the title bar and entering a new title in the widget settings dialog box. Some widgets have more options in their respective settings dialog box.

To reset a widget title to its default name, simply leave the *Custom widget title* field blank.

The widget refresh interval can also be manually adjusted from this dialog box.

System Information widget

The system dashboard includes a *System Information* widget, which displays the current status of the FortiAuthenticator unit and enables you to configure basic system settings.

The following information is available on this widget:

Host Name	The identifying name assigned to this FortiAuthenticator unit. For more information, see Changing the host name on page 25.
DNS Domain Name	The DNS domain name. For more information, see Changing the DNS domain name on page 26.
Serial Number	The serial number of the FortiAuthenticator unit. The serial number is unique to the FortiAuthenticator unit and does not change with firmware upgrades. The serial number is used for identification when connecting to the FortiGuard server.
System Time	The current date, time, and time zone on the FortiAuthenticator internal clock or NTP servers. For more information, see Configuring the system time, time zone, and date on page 26.
Firmware Version	The version number and build number of the firmware installed on the FortiAuthenticator unit. To update the firmware, you must download the latest version from the Customer Service & Support portal at https://support.fortinet.com. Select *Update* and select the firmware image to load from your management computer.
Architecture	The architecture of the device, such as 32-bit.
System Configuration	The date of the last system configuration backup. Select Backup/Restore to backup or restore the system configuration. For more information, see Backing up and restoring the configuration on page 28.
Current Administrator	The name of the currently logged on administrator.
Uptime	The duration of time the FortiAuthenticator unit has been running since it was last started or restarted.
Shutdown/Reboot	Options to shutdown or reboot the device. When rebooting or shutting down the system, you have the option to enter a message that will be added to the event log explaining the reason for the shutdown or reboot.

Changing the host name

The *System Information* widget will display the full host name.

To change the host name:

1. Go to *System* > *Dashboard*.
2. In the *System Information* widget, in the *Host Name* field, select *Change*. The *Edit Host Name* page opens.
3. In the *Host name* field, type a new host name.

The host name may be up to 35 characters in length. It may include US-ASCII letters, numbers, hyphens, and underscores. Spaces and special characters are not allowed.

4. Select *OK* to save the setting.

Changing the DNS domain name

To change the DNS domain name:

1. Go to *System* > *Dashboard*.
2. In the *System Information* widget, in the *DNS Domain Name* field, select *Change*. The *Edit DNS Domain Name* page opens.
3. Type a DNS domain name in the field.
   The DNS domain name identifies the exact location of this server in the DNS hierarchy.
4. Select *OK* to save the setting.

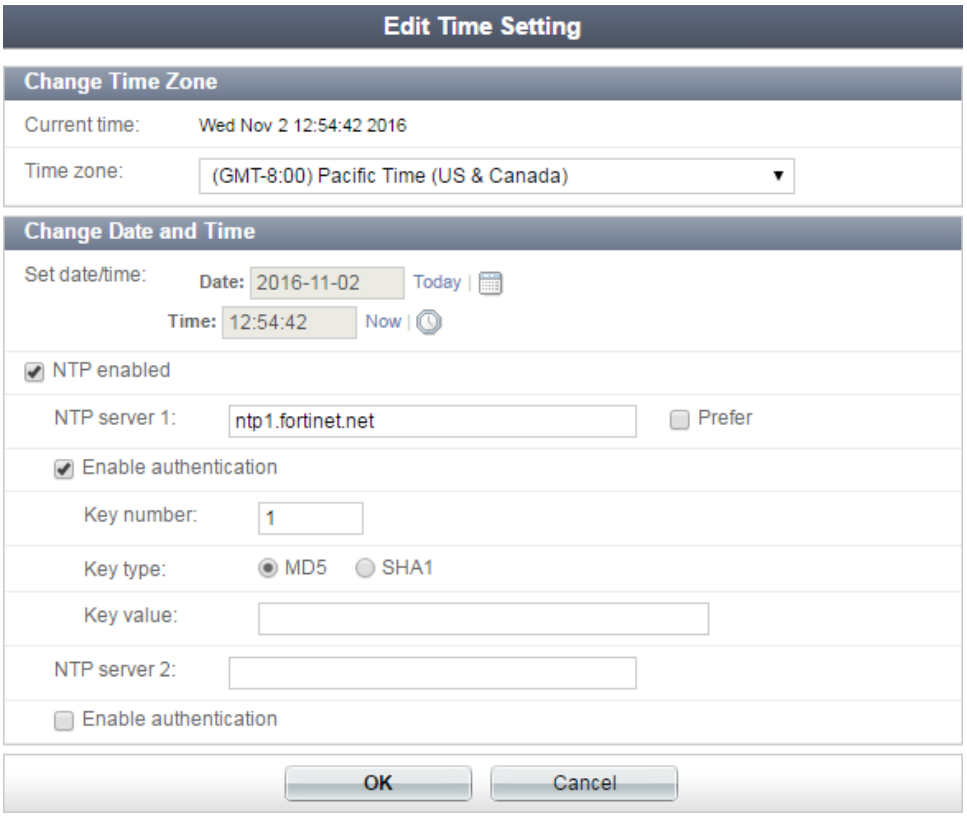
Configuring the system time, time zone, and date

You can either manually set the FortiAuthenticator system time and date, or configure the FortiAuthenticator unit to automatically keep its system time correct by synchronizing with a NTP server.

For many features to work the FortiAuthenticator system time must be accurate. Synchronization with a NTP server is highly recommended.

To configure the date and time:

1. Go to *System* > *Dashboard*.
2. In the *System Information* widget, in the *System Time* field, select *Change*. The *Edit System Time Settings* dialog box appears.



Note that, since the release of FortiAuthenticator 4.2, you can now configure an additional NTP server.

3. Configure the following settings to either manually configure the system time, or to automatically synchronize the FortiAuthenticator unit's clock with a NTP server:

Change Timezone	The host name may be up to 35 characters in length. It may include US-ASCII letters, numbers, hyphens, and underscores. Spaces and special characters are not allowed.
NTP enabled	The host name may be up to 35 characters in length. It may include US-ASCII letters, numbers, hyphens, and underscores. Spaces and special characters are not allowed.
NTP server 1 (or 2)	The host name may be up to 35 characters in length. It may include US-ASCII letters, numbers, hyphens, and underscores. Spaces and special characters are not allowed. Note that, if you configure both NTP servers, you can select the *Prefer* checkbox to make *NTP server 1* the preferred server.
Set date/time	The host name may be up to 35 characters in length. It may include US-ASCII letters, numbers, hyphens, and underscores. Spaces and special characters are not allowed.

4. Select *OK* to apply your changes.

Backing up and restoring the configuration

Fortinet recommends that you back up your FortiAuthenticator configuration to your management computer on a regular basis to ensure that, should the system fail, you can quickly get the system back to its original state with minimal effect to the network. You should also perform a back up after making any changes to the FortiAuthenticator configuration.

The backup file is encrypted to prevent tampering. This configuration file backup includes both the CLI and GUI configurations of the FortiAuthenticator unit. The backed-up information includes users, user groups, FortiToken device list, authentication client list, LDAP directory tree, FSSO settings, remote LDAP, and certificates.

You can perform backups manually. Fortinet recommends backing up all configuration settings from your FortiAuthenticator unit before upgrading the FortiAuthenticator firmware.

Your FortiAuthenticator configuration can also be restored from a backup file on your management computer.

To backup or restore the FortiAuthenticator configuration:

1. Go to *System* > *Dashboard* > *Status*.
2. In the *System Information* widget, in the *System Configuration* field, select *Backup/Restore*. The *Configuration Backup and Restore* page opens.
3. Select from the following settings:

Download backup file	Select *Download backup file* to save a backup file onto the management computer.
Restore File	Select *Browse...* to find the backup file on your management computer, then select *Restore* to restore the selected backup configuration to the device. You will be prompted to confirm the restore action, and the FortiAuthenticator unit will reboot.

4. Select *Cancel* to return to the dashboard page.

When you restore the configuration from a backup file, any information changed since the backup will be lost. Any active sessions will be ended and must be restarted. You will have to log back in when the system reboots.

Restoring a configuration is only possible from a backup file made on the same model running the same version of the operating system.

If you are restoring a configuration on the master device in a HA cluster, shutdown the slave device until the master device is back online to ensure that the configuration synchronization occurs correctly.

System Resources widget

The *System Resources* widget on the dashboard displays the usage status of the CPU and memory as a percentage.

Authentication Activity widget

The *Authentication Activity* widget displays a line graph of the number of logins versus time.

To adjust the data displayed in the graph, select the edit button to open the *Authentication Activity Widget Settings* dialog box.

The following settings are available:

Custom widget title	Enter a custom widget title for the widget, or leave it blank to keep the default title.
Refresh interval	Enter a custom refresh interval for the widget (in seconds), or leave it as the default time of 300 seconds.
Time period	Select a time period for the graph to cover from the drop-down list. The available options are: last 6 hours, last 24 hours, last 3 days, last 7 days, and last 30 days.
Activity Type	Select the activity type to display in the graph. The available options are: All login attempts, Successful login attempts, and Failed login attempts.

User Inventory widget

The *User Inventory* widget displays the numbers of users, groups, FortiTokens, FSSO users, and FortiClient users currently used or logged in, as well as the maximum allowed number, the number still available, and the number that are disabled.

License Information widget

The *License Information* widget displays the device's license information, as well as SMS information. You can also add a license and more SMS messages.

To upload a new license file, select *Upload* in the *License Type* field, then browse to the license file on the management computer.

To add more SMS messages, select *Add Messages* from either the *Sent/Allowed* field or the *Status* field. In the *Add Messages* dialog box, enter the certificate number for the messages and then select *OK* to add the messages.

Top User Lockouts widget

The *Top User Lockouts* widget displays the users who are locked out the most. For more information on user lockouts and for instruction on adjusting user lockout settings, see Lockouts on page 1.

To change the number of user lockouts displayed in the widget, select the edit icon and change the number in the *Number of lockouts* field.

Network

The *Network* tree menu allows you to configure device interfaces, DNS configuration, static routing, and packet capturing.

Interfaces

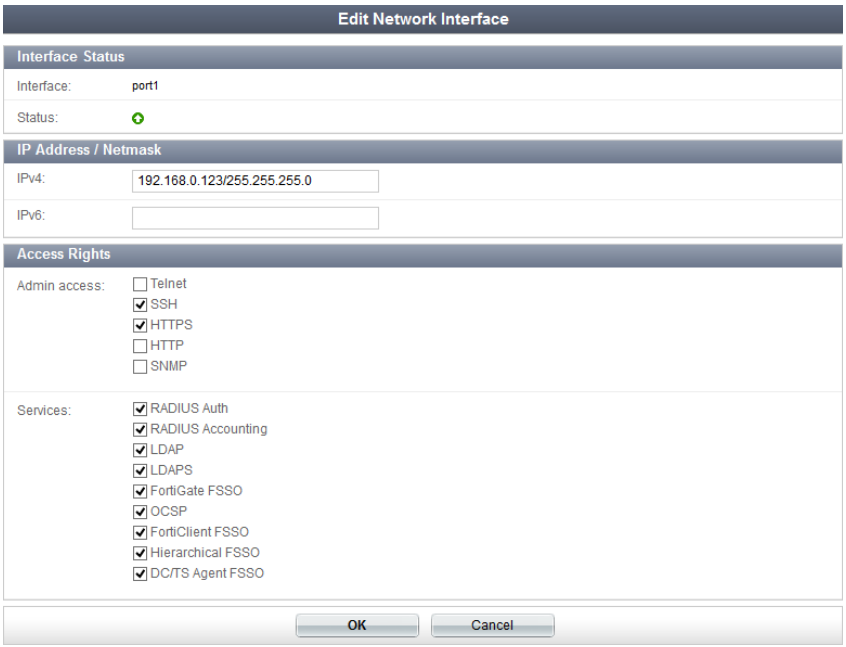
To view the interface list, go to *System* > *Network* > *Interfaces*.

The following information is shown:

Edit	Select to edit the selected interface.
Search	Enter a search term in the search text box then select *Search* to search the interface list.
Interface	The names of the physical interfaces on your FortiAuthenticator unit. The name, including number, of a physical interface depends on the model.
IPv4	The IPv4 address of the interface.
IPv6	The IPv6 address of the interface, if applicable.
Link Status	The link status of the interface.

To edit an interface:

1. In the interfaces list, select the interface you need to edit and select the *Edit* button, or select the interface name. The *Edit Network Interface* window opens.



2. Edit the following settings as required.

Interface Status	The interface name and its current link status is displayed.
IP Address / Netmask	
IPv4	Enter the IPv4 address and netmask associated with this interface.
IPv6	Enter the IPv6 address associated with this interface.
Access Rights	
Admin access	Select the allowed administrative service protocols from: *Telnet*, *SSH*, *HTTPS*, *HTTP*, *SNMP*.
Services	Select the allowed services from: *RADIUS Auth*, *RADIUS Accounting*, *LDAP*, *LDAPS*, *FortiGate FSSO*, *OCSP*, *FortiClient FSSO*, *Hierarchical FSSO*, *DC/TS Agent FSSO*, and *Syslog*. Note: *Syslog* is only available if Syslog SSO has been enabled. See General settings on page 1 for more information.

3. Select *OK* to apply the edits to the network interface.

DNS

To configure DNS settings, go to *System* > *Network* > *DNS*. The primary and secondary nameserver IP addresses can be changed as needed. To apply the changes, select *OK*.

Static routing

To view the list of static routes, go to *System* > *Network* > *Static Routing*. Routes can be created, edited, and deleted as required.

The following information is shown:

Create New	Select to create a new static route.
Delete	Select to delete the selected static route.
Edit	Select to edit the selected static route.
IP/Mask	The destination IP address and netmask for this route.
Gateway	The IP address of the next hop router to which this route directs traffic.
Device	The device or interface associated with this route.

To create a new static route:

1. In the static route list, select *Create New*. The *Create New Static Route* window opens.
2. Edit the following settings as required.

Destination IP/mask	Enter the destination IP address and netmask for this route.
Network interface	Select the network interface that connects to the gateway.
Gateway	Enter the IP address of the next hop router to which this route directs traffic.
Comment	Optionally, enter a comment about the route. Make it fun.

3. Select *OK* to create the new static route.

To edit a static route:

1. In the static route list, select the route you need to edit and then select *Edit*, or click on the route. The *Edit Static Route* window opens.
2. Edit the settings as required, then select *OK* to apply your changes.

To delete a static route:

1. In the static route list, select the route you need to delete.
2. Select *Delete*, then select *OK* in the confirmation dialog box to delete the route.

Packet capture

Packets can be captured on configured interfaces by going to *System* > *Network* > *Packet Capture*.

The following information is available:

Edit	Select to edit the packet sniffer on the selected interface.
Interface	The name of the configured interface for which packets can be captured. For information on configuring an interface, see Interfaces on page 30.
Max packets to capture	The maximum number of packets that can be captured.

Status	The status of the packet capture process. Allows you to start and stop the capturing process, and download the most recently captured packets.

To start capturing packets on an interface, select the *Start capturing* button for that interface. The *Status* will change to *Capturing*, and the *Stop capturing* and download buttons will become available.

To download captured packets:

1. Select the download button for the interface whose captured packets you are downloading.
   If no packets have been captured for that interface, select the *Start capturing* button.
2. When prompted, save the packet file (*sniffer_[interface].pcap*) to your management computer.
   The file can then be opened using packet analyzer software.

To edit a packet sniffer:

1. Select the interface whose packet capture settings you need to configure by either selecting the configured interface name from the interface list, or selecting the checkbox in the interface row and selecting *Edit* from the toolbar.
   The *Edit Packet Sniffer* page opens.
2. Configure the following options:

Interface	The interface name.
Max packets to capture	Enter the maximum number of packets to capture. The default is 500 packets.
Include IPv6 packets	Select to include IPv6 packets when capturing packets.
Include non-IP packets	Select to include non-IP packets when capturing packets.

3. Select *OK* to apply your changes.

Administration

Configure administrative settings for the FortiAuthenticator device. This section includes:

- System Access
- High Availability
- Firmware Upgrade
- Config Auto-backup
- SNMP
- Licensing
- FortiGuard
- FTP Servers
- Admin Profiles

System Access

To adjust system access settings, go to *System* > *Administration* > *System Access*. The *Edit System Access Settings* page will open.

The following settings are available:

Pre-Authentication		Enable pre-authentication warning message. These can be found under *Authentication* > *Self-service Portal* > *Replacement Messages*.
CLI Access		
	CLI idle timeout	Enter the amount of time before the CLI times out due to inactivity, from 0 to 480 minutes.
GUI Access		

	GUI idle timeout	Enter the amount of time before the GUI times out due to inactivity, from 1 to 480 minutes.
	Maximum HTTP header length	Enter the maximum HTTP header length, from 4 to 16 KB.
	HTTPS Certificate	Select an HTTPS certificate from the drop-down list.
	Certificate authority type	Select the selected certificate's authority type, either *Local CA* or *Trusted CA*.
	CA certificate that issued the server certificate	Select the issuing server certificate from the drop-down list.
	Additional allowed hosts/domain names	Specify any additional hosts that this site can serve, separated by commas or line breaks.
	IP/FQDN	Enter the IP, or FQDN, of the FortiAuthenticator for external access.
RESTful API Access		
	Restrict web service access to a specific interface	When enabled, select an available interface from the dropdown menu.

Select *OK* to apply any changes. See Certificate Management on page 1 for more information about certificates.

High Availability

Multiple FortiAuthenticator units can operate as a cluster to provide even higher reliability, called HA.

There are three HA roles:

- Cluster member
- Standalone master
- Load-balancing slave

The FortiAuthenticator can operate in two separate HA modes:

- Cluster : Active-passive clustered fail-over mode where all of the configuration is synchronized between the devices.
- Load-balancing: Active-active HA method in which one device acts as a standalone master with up to two additional, geographically separated load-balancing slaves. The load can be distributed across the devices using round-robin DNS, Auth/NAS client load distribution, or external load balancing devices. Load-balancing mode is

intended for two-factor authentication deployments, as only a subset of the configuration is synchronized between the devices.

Both HA modes can be combined with a HA cluster acting as a standalone master for geographically distributed load-balancing slaves.

If a HA cluster is configured on an interface (such as port 2) and then disabled, it will not be possible to re-enable HA.
This is because, when disabled, the interface's IP address is reconfigured to the interface to allow the administrator to access the newly standalone device. To allow the port to be available for use again in a HA cluster, the IP address must be manually removed.

Cluster member role

In the cluster member role, one unit is active and the other is on standby. If the active unit fails, the standby unit becomes active. The cluster is configured as a single authentication server on your FortiGate units.

Authentication requests made during a failover from one unit to another are lost, but subsequent requests complete normally. The failover process takes about 30 seconds.

Cluster mode uses Ethernet broadcasts through TCP port 720 as part of its master/slave election mechanism and for ongoing communication. Layer 2 connectivity is required between the two devices in a HA cluster, preferably via a crossover cable, as some network devices might block such Ethernet broadcasts.

To configure FortiAuthenticator HA

1. On each unit, go to *System* > *Administration* > *High Availability*
2. Enter the following information:

Enable HA	Enable HA.
Role	Select *Cluster member*.
Interface	Select a network interface to use for communication between the two cluster members. This interface must not already have a IP address assigned and it cannot be used for authentication services. Both units must use the same interface for HA communication.
Cluster member IP address	Enter the IP address this unit uses for HA-related communication with the other FortiAuthenticator unit. The two units must have different addresses. Usually, you should assign addresses on the same private subnet.
Admin access	Select the types of administrative access to allow from: *Telnet*, *SSH*, *HTTPS*, *HTTP*, and *SNMP*.
Priority	Set to *Low* on one unit and *High* on the other. Normally, the unit with High priority is the master unit.
Password	Enter a string to be used as a shared key for IPsec encryption. This must be the same on both units.

3. Select *OK* to apply the settings.

When one unit has become the master, reconnect to the GUI and complete your configuration. The configuration will automatically be copied to the slave unit.

Standalone master and Load-balancing slave roles

The load-balancing HA method enables active-active HA across geographically separated locations and layer 3 networks. Only the following authentication related features can be synchronized:

- Token and seeds
- Local user database
- Remote user database
- Group mappings
- Token and user mappings

Other features, such as FSSO and certificates, cannot be synchronized between devices.

The standalone master is the primary system where users, groups, and tokens are configured. The load-balancing slave is synchronized to the master.

To improve the resilience of the master system, an active-passive master cluster with up to two load-balancing slave devices can be configured.

Remote administrator users are not synchronized between the Master and the load-balancing slave.

As a workaround, you can import remote users to slave roles, and change their roles to Administrator.

To configure load-balancing HA

1. On each unit, go to *System* > *Administration* > *High Availability*
2. Enter the following information:

Enable HA	Enable HA.
Role	Select *Standalone master* on the master device, and *Load-balancing slave* on the slave device or devices.
Password	Enter a string to be used as a shared key for IPsec encryption. This must be the same on both units.
Load-balancing slaves	On the master, enter IP address or IP addresses of the load-balancing slave devices. Up to two can be added.

3. Select *OK* to apply the settings.

To configure HA automatic session pickup

1. On the master, go to *System* > *Administration* > *High Availability* and edit the settings:

Monitored interfaces	Select an interface connected to a slave device. If this interface goes down, the HA interface will be automatically brought down.
Monitored interfaces stability period	Enter a period of time in seconds to wait before the interface is brought back up once connectivity returns. This delay time is to ensure that the port is connected correctly. Set the value between 0-3600.

2. Select *OK* to apply the settings.

Administrative access to the HA cluster

Administrative access is available through any of the network interfaces using their assigned IP addresses or through the HA interface using the *Cluster member IP address*, assigned on the *System* > *Administration* > *High Availability* page. In all cases, administrative access is available only if it is enabled on the interface.

Administrative access through any of the network interface IP addresses connects only to the master unit. The only administrative access to the slave unit is through the HA interface using the slave unit's *Cluster member IP address*.

Configuration changes made on the master unit are automatically pushed to the slave unit. The slave unit does not permit configuration changes, but you might want to access the unit to change HA settings, or for firmware upgrades, shutdown, reboot, or troubleshooting.

FortiAuthenticator VMs used in a HA cluster each require a license. Each license is tied to a specific IP address. In a HA cluster, all interface IP addresses are the same on the two units, except for the HA interface. Request each license based on either the unique IP address of the unit's HA interface or the IP address of a non-HA interface which will be the same on both units.

If you disable and then re-enable HA operation, the interface that was assigned to HA communication will not be available for HA use. You must first go to *System* > *Network* > *Interfaces* and delete the IP address from that interface.

Restoring the configuration

When restoring a configuration to a HA cluster master device, the master will reboot and in the interim the slave device will be promoted to master. When the previous master returns to service, it will become a slave and the existing master will overwrite its configuration, defeating the configuration restore. To avoid this, use the following process when restoring a configuration:

1. Shutdown the slave unit.
2. Restore the configuration on the master unit.
3. Wait until the master unit is back online.
4. Turn on slave unit — it will synchronize to the restored configuration after booting up.

Firmware upgrade

For a stable HA configuration, all units in a HA cluster must be running the same firmware version, and have the same sized license for HA devices.

When upgrading the firmware on FortiAuthenticator devices in an HA cluster, specific steps must be taken to ensure that the upgrade is successful:

1. Start the firmware upgrade on the active, or master, device. See Upgrading the firmware on page 1.

   The device will reboot. While the master device is rebooting, the standby, or slave, device becomes the master.

2. Start the firmware upgrade on the new master device.

   The device will reboot.

   Once both devices have rebooted, the original master device will again be the master, while the slave device will return to being the slave.

If a situation arises where both devices are claiming to be the HA master due to a firmware mismatch, and the HA port of the device that is intended to be the slave cannot be accessed (such as when a crossover cable is being used), use the following steps:

1. Shutdown the master device to which you have access, or, if physical access to the unit is not available to turn it back on, reboot the device. See System Information widget.

   Note that, if rebooting the device, Step 2 must be completed before the device finishes rebooting, which is can be as short as 30 seconds.

2. With the previously inaccessible device now accessible, upgrade its firmware to the required version so that both devices have the same version.

   The device will reboot.

3. If you shutdown the device in Step 1, power it back on.

   Once both devices are back online, they will assume the HA roles dictated by their respective HA priorities.

Firmware Upgrade

The FortiAuthenticator firmware can be upgraded by either going to *System* > *Administration* > *Firmware*, or through the *System Information* widget of the dashboard (see System Information widget on page 1).

For instructions on upgrading the device's firmware, see Upgrading the firmware on page 1.

Upgrade history

The upgrade history of the device is shown under the *Upgrade History* heading in the *Firmware Upgrade or Downgrade* pane. It displays the version that was upgraded to, the time and date that the upgrade took place, and the user that performed the upgrade. This information can be useful when receiving support to identify incorrect upgrade paths that can cause stability issues.

Always review all sections in the *FortiAuthenticator Release Notes* prior to upgrading your device.

Config Auto-backup

You can configure the FortiAuthenticator to automatically back up the configuration of the FortiAuthenticator unit to an FTP or SFTP server.

Even though the backup file is encrypted to prevent tampering, access to the FTP server should be restricted. This configuration file backup includes both the CLI and GUI configurations of the FortiAuthenticator unit. The backed-up information includes users, user groups, FortiToken device list, authentication client list, LDAP directory tree, FSSO settings, remote LDAP and RADIUS, and certificates.

To configure automatic backups, go to *System* > *Administration* > *Config Auto-backup*.

Enter the following information, and then select *OK* to apply the settings:

Enable configuration auto-backup	Enable the configuration of automatic configuration backups.
Frequency	Select the automatic backup frequency, one of: *Hourly*, *Daily*, *Weekly*, or *Monthly*.
Backup time	Entire a time for the backups to occur, or select the clock icon and select from the drop-down menu. You can also select *Now* to set the scheduled time to the current time. This options is not available when the frequency is set to hourly.
FTP directory	Enter the FTP directory where the backup configuration files will be saved.
FTP server	Select the FTP server to which the backup configuration files will be saved. See FTP Servers on page 45 for information on adding FTP servers.
Secondary FTP server	Select a secondary FTP server.

SNMP

Simple Network Management Protocol (SNMP) enables you to monitor hardware on your network. You can configure the hardware, such as the FortiAuthenticator SNMP agent, to report system information and send traps (alarms or event messages) to SNMP managers. An SNMP manager, or host, is typically a computer running an application that can read the incoming trap and event messages from the agent, and send out SNMP queries to the SNMP agents.

By using an SNMP manager, you can access SNMP traps and data from any FortiAuthenticator interface configured for SNMP management access. Part of configuring an SNMP manager is listing it as a host in a community on the FortiAuthenticator unit it will be monitoring. Otherwise, the SNMP monitor will not receive any traps from that unit, or be able to query that unit.

The FortiAuthenticator SNMP implementation is read-only. SNMP v1, v2c, and v3 compliant SNMP managers have read-only access to system information through queries and can receive trap messages from the FortiAuthenticator unit.

To monitor FortiAuthenticator system information and receive FortiAuthenticator traps, your SNMP manager needs the Fortinet and FortiAuthenticator Management Information Base (MIB) files. A MIB is a text file that lists the SNMP data objects that apply to the device to be monitored. These MIBs provide information that the SNMP

manager needs to interpret the SNMP trap, event, and query messages sent by the FortiAuthenticator unit SNMP agent.

The Fortinet implementation of SNMP includes support for most of RFC 2665 (Ethernet-like MIB) and most of RFC 1213 (MIB II). RFC support for SNMP v3 includes Architecture for SNMP Frameworks (RFC 3411), and partial support of User-based Security Model (RFC 3414).

SNMP traps alert you to important events that occur, such as overuse of memory or a high rate of authentication failures.

SNMP fields contain information about the FortiAuthenticator unit, such as CPU usage percentage or the number of sessions. This information is useful for monitoring the condition of the unit on an ongoing basis and to provide more information when a trap occurs.

Configuring SNMP

Before a remote SNMP manager can connect to the Fortinet agent, you must configure one or more interfaces to accept SNMP connections by going to *System* > *Network* > *Interfaces*. Select the interface, and in *Administrative Access*, select *SNMP*. See Interfaces on page 1.

You can also set the thresholds that trigger various SNMP traps. Note that a setting of zero disables the trap.

To configure SNMP settings:

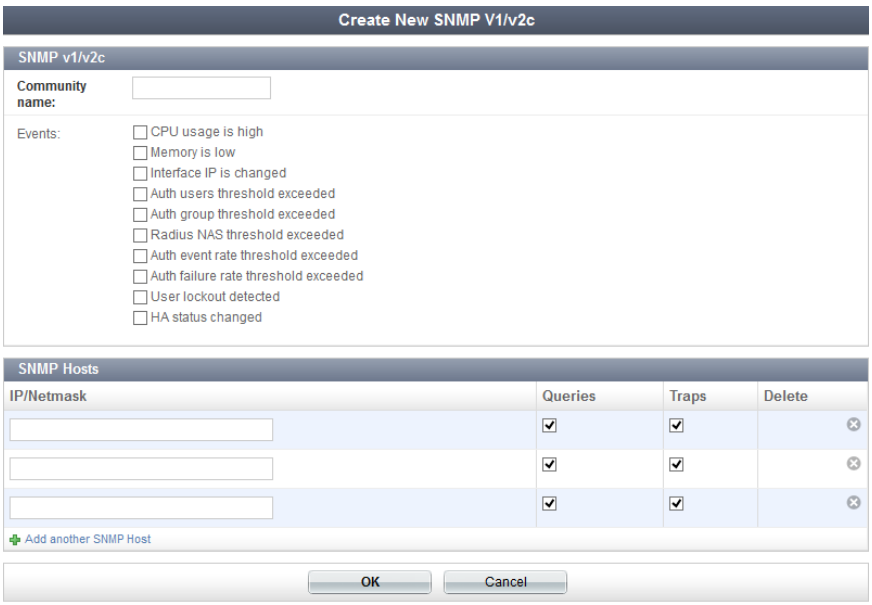
1. Go to *System* > *Administration* > *SNMP*.
2. Enter the following information:

SNMP Contact	Enter the contact information for the person responsible for this FortiAuthenticator unit.
SNMP Description	Enter descriptive information about the FortiAuthenticator unit.
SNMP Location	Enter the physical location of the FortiAuthenticator unit.
User Table Nearly Full Trap Threshold	The user table is nearly full. The threshold is a percentage of the maximum permitted number of users.
User Group Table Nearly Full Trap Threshold	The user group table is nearly full. The threshold is a percentage of the maximum permitted number of user groups.
RADIUS Auth Client Table Nearly Full Trap Threshold	The RADIUS authenticated client table is nearly full. The threshold is a percentage of the maximum permitted number of RADIUS clients.
Auth Event Rate Over Limit Trap Threshold	High authentication load. The threshold is the number of authentication events over a 5-minute period.
Auth Failure Rate Over Limit Trap Threshold	High rate of authentication failure. The threshold is the number of authentication failures over a 5-minute period.
CPU Utilization Trap Threshold (%)	High load on CPU. Default 90%.
Disk Utilization Trap Threshold (%)	Disk usage is high. Default 80%.
Memory Utilization Trap Threshold (%)	Too much memory used. Default 90%.

3. Select *OK* to apply the changes.

To create a new SNMP community:

1. Go to *System* > *Administration* > *SNMP.*
2. Select *Create New* under *SNMP v1/v2c*. The *Create New SNMP V1/v2c* window opens.



3. Enter the following information in the *SNMPv1/v2c* section:

Community	The name of the SNMP community.
Events	**Select the events for which traps are enabled. Options include:** • CPU usage is high • Memory is low • Interface IP is changed • Auth users threshold exceeded • Auth group threshold exceeded • Radius NAS threshold exceeded • Auth event rate threshold exceeded • Auth failure rate threshold exceeded • User lockout detected. • HA status is changed

4. In *SNMP Hosts*, select *Add another SNMP Host* and enter the following information:

IP/Netmask	Enter the IP address and netmask of the host.
Queries	Select if this host uses queries.
Traps	Select if this host uses traps.
Delete	Select to delete the host.

5. Select *OK* to create the new SNMP community.

To create a new SNMP user:

1. Go to *System* > *Administration* > *SNMP.*
2. Select *Create New* under *SNMP v3*. The *Create New SNMP V3* window opens.
3. Enter the following information in the *General* section:

Username	The name of the SNMP user.
Security Level	Select the security level from the drop-down list: • *None*: no authentication or encryption • *Authentication only*: select the *Authentication method* then enter the authentication key in the *Authentication key* field • *Encryption and authentication*: select the *Authentication method*, enter the authentication key in the *Authentication key* field, then select the *Encryption method* and enter the encryption key in the *Encryption key* field.
Events	Select the events for which traps are enabled. See Events on page 42.

4. In *SNMP Notification Hosts*, select *Add another SNMP Notification Host* and enter the following information:

IP/Netmask	Enter the IP address and netmask of the notification host.
Delete	Select to delete the notification host.

5. Select *OK* to create the new SNMP V3 user.

To download MIB files:

1. Go to *System* > *Administration* > *SNMP*.
2. Under *FortiAuthenticator SNMP MIB*, select the MIB file you need to download, options include the Fortinet Core MIB and the FortiAuthenticator MIB files.

   The selected MIB file is downloaded to your computer.

Licensing

FortiAuthenticator-VM works in evaluation mode until it is licensed. In evaluation mode, only a limited number of users can be configured on the system. To expand this capability, a stackable licence can be applied to the system to increase both the user count, and all other metrics associated with the user count.

When a license is purchased, a registration code is provided. Go to support.fortinet.com and register your device by entering the registration code. You will be asked for the IP address of your FortiAuthenticator unit, and will then be provided with a license key.

Ensure that the IP address specified while registering your unit is configured on one of the device's network interfaces, then upload the license key to your FortiAuthenticator-VM.

The *License Information* widget shows the current state of the device license. See License Information widget on page 1.

To license FortiAuthenticator:

1. Register your device.
2. Ensure that one of your device's network interfaces is configured to the IP address specified during registration.
3. Go to *System* > *Administration* > *Licensing*.
4. Select *Browse...* and locate, on your local computer, the license file you received from Fortinet.
5. Select *OK*.

FortiGuard

To view and configure FortiGuard connections, go to *System* > *Administration* > *FortiGuard*. The FortiGuard Distribution Network (FDN) page provides information and configuration settings for FortiGuard subscription services. For more information about FortiGuard services, see the FortiGuard Center web page (http://www.fortiguardcenter.com).

Configure the following settings, then select *OK* to apply them:

FortiGuard Subscription Services		
	Messaging Service	The data to which the messaging service license is valid.
	SMS messages	The total number of allowed SMS messages, and the number of messages that have been used.
ForttiGuard Proxy Server		
	Enable FortiGuard proxy server	If enabled, communication with FortiGuard servers will go through this proxy server.
FortiToken Hardware Provisioning		
	Server address	The server address.
FortiToken Mobile Provisioning		
	Server address	The server address.
	Server port	The server port.
	Activation timeout	The activation timeout in hours, from 1 to 168 hours.
	Token size	The token size, either 6 or 8.
	Time step	The time step, either 60 or 30.
	Require PIN	Select to require a PIN.
FortiGuard Messaging Service		

Server address	The server address.
Server port	The server port.

FTP Servers

To view a list of the configured FTP servers, go to *System* > *Administration* > *FTP Servers*.

The following information is shown:

Create New	Select to create a new FTP server.
Delete	Select to delete the selected FTP server or servers.
Edit	Select to edit the selected FTP server.
Name	The name of the FTP server.
Server name/IP	The server name or IP address, and port number.

To create a new FTP server:

1. Select *Create New*. The *Create New FTP Server* window will open.
2. Enter the following information:

Name	Enter a name for the FTP server.
Connection type	Select the connection type, either *FTP* or *SFTP*.
Server name/IP	Enter the server name or IP address.
Port	Enter the port number.
Anonymous	Select to make the server anonymous.
Username	Enter the server username (if *Anonymous* is not selected).
Password	Enter the server password (if *Anonymous* is not selected).

3. Select *OK* to create the new FTP server.

Admin Profiles

Similar to FortiOS, FortiAuthenticator can incorporate the use of admin profiles. Each administrator can be granted either full permissions or a customized admin profile. Profiles are defined as aggregates of read-only or read/write permission sets. The most commonly used permission sets are pre-defined, but custom permission sets can also be created.

To create a new admin profile, go to *System* > *Admin Profiles* > *Manage* > *Create New*. You can give the admin profile a name, a description, and configure the permission sets you want for that particular admin profile.

Go to *Authentication* > *User Management* > *Local Users*, and select the admin profile to an administrator. You can assign more than one admin profile to each administrator.

Messaging

The FortiAuthenticator unit sends email for several purposes, such as password reset requests, new user approvals, user self-registration, and two-factor authentication.

By default, the FortiAuthenticator unit uses its built-in Simple Mail Transfer Protocol (SMTP) server. This is provided for convenience, but is not necessarily optimal for production environments. Fortinet recommends that you configure the unit to use a reliable external mail relay.

There are two distinct email services:

- Administrators - password reset, new user approval, two-factor authentication, etc.
- Users - password reset, self-registration, two-factor authentication, etc.

If you will be sending SMS messages to users, you must configure the SMS gateways that you will use. Ask your SMS provider for information about using its gateway. The FortiAuthenticator SMS gateway configuration differs according to the protocol your SMS provider uses.

SMTP Servers

To view a list of the SMTP servers, go to *System* > *Messages* > *SMTP Servers*.

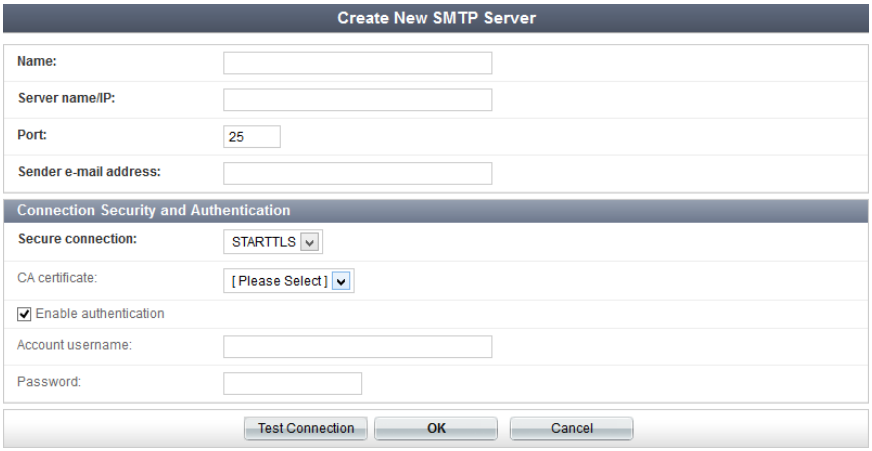
Although the FortiAuthenticator can be configured to send emails from the built-in mail server (localhost), this is not recommended. Anti-spam methods such as IP lookup, DKIM, and SPF can cause mail from such ad-hoc mail servers to be blocked. It is highly recommended that email is relayed via an official mail server for your domain.

The following information is shown:

Create New	Select to create a new SMTP server.
Delete	Select to delete the selected SMTP server or servers.
Edit	Select to edit the selected SMTP server.
Set as Default	Set the selected SMTP server as the default SMTP server.
Name	The name of the SMTP server.
Server	The server name and port number.
Default	Shows a green circle with a check mark for the default SMTP server. To change the default server, select the server you would like to use as the default, then select *Set as Default* in the toolbar.

To add an external SMTP server:

1. Go to *System* > *Messages* > *SMTP Servers* and select *Create New*. The *Create New SMTP Server* window opens.



2. Enter the following information:

Name	Enter a name to identify this mail server on the FortiAuthenticator unit.
Server Name/IP	Enter the IP address or Fully Qualified Domain Name (FQDN) of the mail server.
Port	The default port 25. Change it if your SMTP server uses a different port.
Sender e-mail address	In the From field, enter the email address that will appear when sending an email from the FortiAuthenticator unit.
Secure connection	For a secure connection to the mail server, select *STARTTLS* from the drop-down list, then select the CA certificate that validates the server's certificate. For information about importing the CA certificate, see Importing CA certificates and signing requests on page 1.
Enable authentication	Select if the email server requires you to authenticate when sending email. Enter the *Account username* and *Password* if required.

3. Optionally, select *Test Connection* to send a test email message. Specify a recipient and select *Send*. Confirm that the recipient received the message.

The recipient's email system might treat the test email message as spam.

4. Select *OK* to create the new SMTP server.

E-mail Services

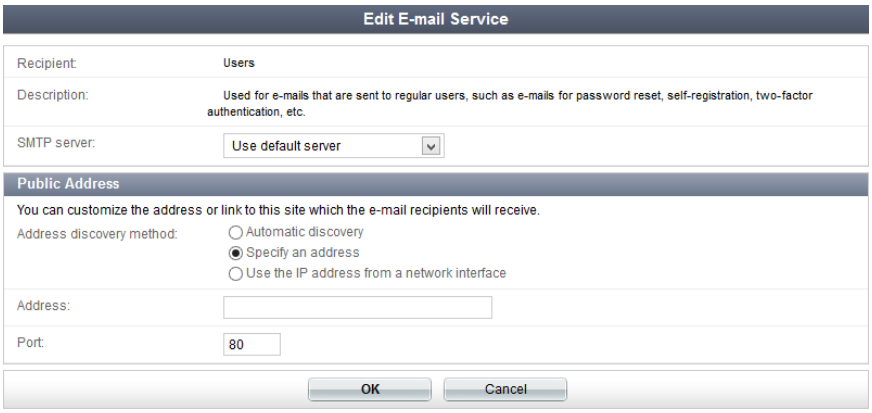
To view a list of the email services, go to *System* > *Messages* > *E-mail Services*.

The following information is shown:

Edit	Select to edit the selected email service.
Recipient	The name of the email recipient.
SMTP server	The SMTP server associated with the recipient. The server can be selected from the drop-down list.
Save	Select to save any changes made to the email services.

To configure email services:

1. Go to *System* > *Messages* > *E-mail Services* and select the recipient you need to edit. The *Edit E-mail Service* window opens.



2. Configure the following:

SMTP Server	Select the SMTP server from the drop-down list.
Public Address	Customize the address or link for the email.
Address discovery method	Select the address discover method: • *Automatic Discovery*: Use DNS domain name if configured, or automatically obtain address from the browser or an active network interface. • *Specify an address*: Manually enter the address and port number. • *Use the IP address from a network interface*: Select a specific network interface from the drop-down list.
Address	Enter the recipient address. Only available if *Address discovery method* is set to *Specify an Address*.
Port	Enter the recipient port number. Only available if *Address discovery method* is set to *Specify an Address*.
Network interface	Select a configured network interface from the drop-down list. This option is only available when the *Address discovery method* is set to *Use the IP address from a network interface*.

3. Select *OK* to apply your changes.

SMS Gateways

To view a list of the configured SMS gateways, go to *System* > *Messages* > *SMS Gateways*.

The following information is shown:

Create New	Select to create a new SMS gateway.
Delete	Select to delete the selected SMS gateway or gateways.
Edit	Select to edit the selected SMS gateway.
Set as Default	Set the selected SMS gateway as the default SMS gateway.
Name	The name of the SMS gateway.
Protocol	The protocol used by the gateway.
SMTP server	The SMTP server associated with the gateway.
API URL	The gateway's API URL, if it has one.
Default	Shows a green circle with a check mark for the default SMS gateway. To change the default gateway, select the gateway you would like to use as the default, then select *Set as Default* in the toolbar.

You can also configure the message that you will send to users. You can use the following tags for user-specific information:

Tag	Information
{{:country_code}}	Telephone country code, e.g. 01 for North America.
{{:mobile_number}}	User's mobile phone number.
{{:message}}	"Your authentication token code is " and the code.

To create a new SMTP SMS gateway:

1. Go to *System* > *Messages* > *SMS Gateways* and select *Create New*. The *Create New SMS Gateway* window opens.

2. Enter the following information:

Name	Enter a name for the new gateway.
Protocol	Select SMTP.
SMTP server	Select the SMTP server you use to contact the SMS gateway. The SMTP server must already be configured, see SMTP Servers on page 46.
Mail-to-SMS gateway	Change `domain.com` to the SMS provider's domain name. The default entry `{{:mobile_number}}@domain.com` assumes that the address is the user's mobile number followed by @ and the domain name. In the *E-mail Preview* field, check the *To* field to ensure that the format of the address matches the information from your provider.
Subject	Optionally, enter a subject for the message.
Body	Optionally, enter body text for the message.
E-mail Preview	View a preview of the email message.

3. Optionally, select *Test Settings* to send a test SMS message to the user.
4. Select *OK* to create a new SMTP SMS gateway.

To create a new HTTP or HTTPS SMS gateway:

1. Go to *System* > *Messages* > *SMS Gateways* and select *Create New*. The *Create New SMS Gateway* window opens.
2. Expand the *HTTP/HTTPS* section, then enter the following information:

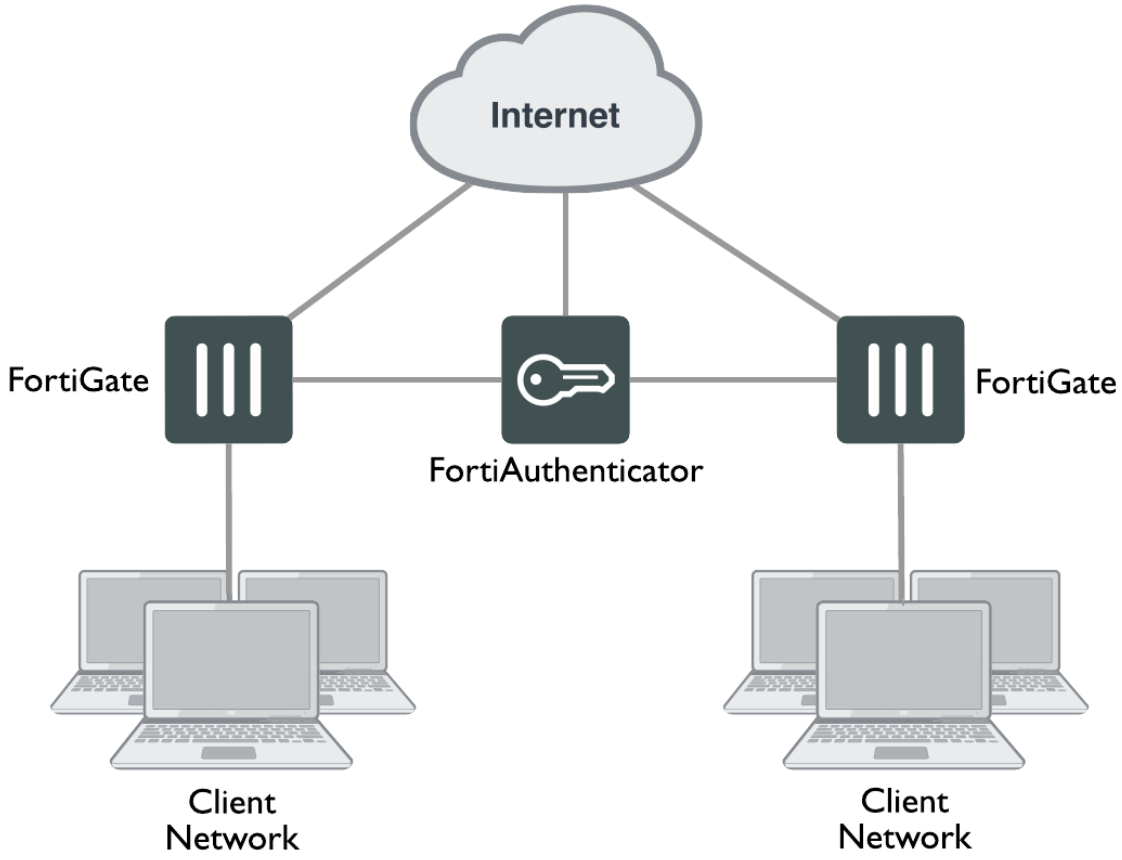
Name	Enter a name for the new gateway.
Protocol	Select HTTP or HTTPS.
HTTP/HTTPS	
HTTP method	Select the method to use, either *GET* of *POST*.
API URL	Enter the gateway URL, omitting the protocol prefix `http://` or `https://`. Also omit the parameter string that begins with `?`.
CA certificate	Select CA certificate that validates this SMS provider from the drop-down list. This option is only available if *Protocol* is set to *HTTPS*.
HTTP Parameters	
Field	Enter the parameter names that the SMS provider's URL requires, such as `user` and `password`.
Value	Enter the values or tags corresponding to the fields.
Delete	Delete the field and its value.

3. If you need more parameter entries, select *Add another SMS Gateway HTTP Parameter.*
4. Optionally, select *Test Settings* to send a test SMS message to the user.
5. Select *OK* to create a new HTTP or HTTPS SMS gateway.

Authentication

FortiAuthenticator provides an easy to configure authentication server for your users. Multiple FortiGate units can use a single FortiAuthenticator unit for remote authentication and FortiToken device management.

FortiAuthenticator in a multiple FortiGate unit network



This chapter includes the following topics:

- SAML IdP
- FortiAuthenticator Agent

What to configure

You need to decide which elements of FortiAuthenticator configuration you need.

- Determine the type of authentication you will use: password-based or token-based. Optionally, you can enable both types. This is called two-factor authentication.
- Determine the type of authentication server you will use: RADIUS, built-in LDAP, or Remote LDAP. You will need to use at least one of these server types.
- Determine which FortiGate units or third party devices will use the FortiAuthenticator unit. The FortiAuthenticator unit must be configured on each FortiGate unit as an authentication server, either RADIUS or LDAP. For RADIUS authentication, each FortiGate unit or third party device must be configured on the FortiAuthenticator unit as an authentication client.

Password-based authentication

User accounts can be created on the FortiAuthenticator device in multiple ways:

- Administrator creates a user and specifies their username and password.
- Administrator creates a username and a random password is automatically emailed to the user.
- Users are created by importing either a CSV file or from an external LDAP server.

Users can self-register for password-based authentication. This reduces the workload for the system administrator. Users can choose their own passwords or have a randomly generated password provided in the browser or sent to them via email or SMS. Self-registration can be instant, or it can require administrator approval. See Self-registration on page 1.

Once created, users are automatically part of the RADIUS Authentication system and can be authenticated remotely.

See User management on page 1 for more information about user accounts.

Two-factor authentication

Two-factor authentication increases security by requiring multiple pieces of information on top of the username and password. There are generally two factors:

- something the user knows, usually a password,
- something the user has, such as a FortiToken device.

Requiring the two factors increases the difficulty for an unauthorized person to impersonate a legitimate user.

To enable two-factor authentication, configure both password-based and token-based authentication in the user's account.

FortiAuthenticator token-based authentication requires the user to enter a numeric token at login. Two types of numerical tokens are supported:

- Time based: TOTP (RFC 6238)

  The token passcode is generated using a combination of the time and a secret key which is known only by the token and the FortiAuthenticator device. The token password changes at regular time intervals, and the FortiAuthenticator unit is able to validate the entered passcode using the time and the secret seed information for that token.

  Passcodes can only be used a single time (one time passcodes) to prevent replay attacks. Fortinet has the following time based tokens:

  - FortiToken hardware
  - FortiToken Mobile, running on a compatible smartphone

- Event based: HMAC-based One Time Password (HTOP) (RFC 4226)

  The token passcode is generated using an event trigger and a secret key. Event tokens are supported using a valid email account and a mobile phone number with SMS service.

  FortiToken devices, FortiToken Mobile apps, email addresses, and phone numbers must be configured in the user's account.

  Only the administrator can configure token-based authentication. See Configuring token based authentication on page 1.

Authentication servers

The FortiAuthenticator unit has built-in RADIUS and LDAP servers. It also supports the use of remote RADIUS and LDAP (which can include Windows AD servers).

The built-in servers are best used where there is no existing authentication infrastructure, or when a separate set of credentials is required. You build a user account database on the FortiAuthenticator unit. The database can include additional user information such as street addresses and phone numbers that cannot be stored in a FortiGate unit's user authentication database. To authenticate, either LDAP or RADIUS can be used. The remote LDAP option adds your FortiGate units to an existing LDAP structure. Optionally, you can add two-factor authentication to remote LDAP.

RADIUS

If you use RADIUS, you must enable RADIUS in each user account. FortiGate units must be registered as RADIUS authentication clients in *Authentication* > *RADIUS Service* > *Clients*. See RADIUS service on page 1. On each FortiGate unit that will use the RADIUS protocol, the FortiAuthenticator unit must be configured as a RADIUS server in *User & Device* > *Authentication* > *RADIUS Server*.

Built-in LDAP

If you use built-in LDAP, you will need to configure the LDAP directory tree. You add users from the user database to the appropriate nodes in the LDAP hierarchy. See Creating the directory tree on page 1. On each FortiGate unit that will use LDAP protocol, the FortiAuthenticator unit must be configured as an LDAP server in *User & Device* > *Authentication* > *LDAP Server*.

Remote LDAP

Remote LDAP is used when an existing LDAP directory exists and should be used for authentication. User information can be selectively synchronized with the FortiAuthenticator unit, but the user credentials (passwords) remain on, and are validated against the LDAP directory.

To utilize remote LDAP, the authentication client (such as a FortiGate device) must connect to the FortiAuthenticator device using RADIUS to authenticate the user information (see *User & Device > Authentication > RADIUS Server*). The password is then proxied to the LDAP server for validation, while any associated token passcode is validated locally.

Machine authentication

Machine, or computer, authentication is a feature of the Windows supplicant that allows a Windows machine to authenticate to a network via 802.1X prior to user authentication.

Machine authentication is performed by the computer itself, which sends its computer object credentials before the Windows logon screen appears. User authentication is performed after the user logs in to Windows.

Based on the computer credentials provided during machine authentication, limited access to the network can be granted. For example, access can be granted to just the Active Directory server to enable user authentication.

Following machine authentication, user authentication can take place to authenticate that the user is also valid, and to then grant further access to the network.

Machine authentication commonly occurs on boot up or log out, and not, for example, when a device awakens from hibernation. Because of this, the FortiAuthenticator caches authenticated devices based on their MAC addresses for a configurable period (see General on page 1). For more information on cached users, see Windows device logins on page 1

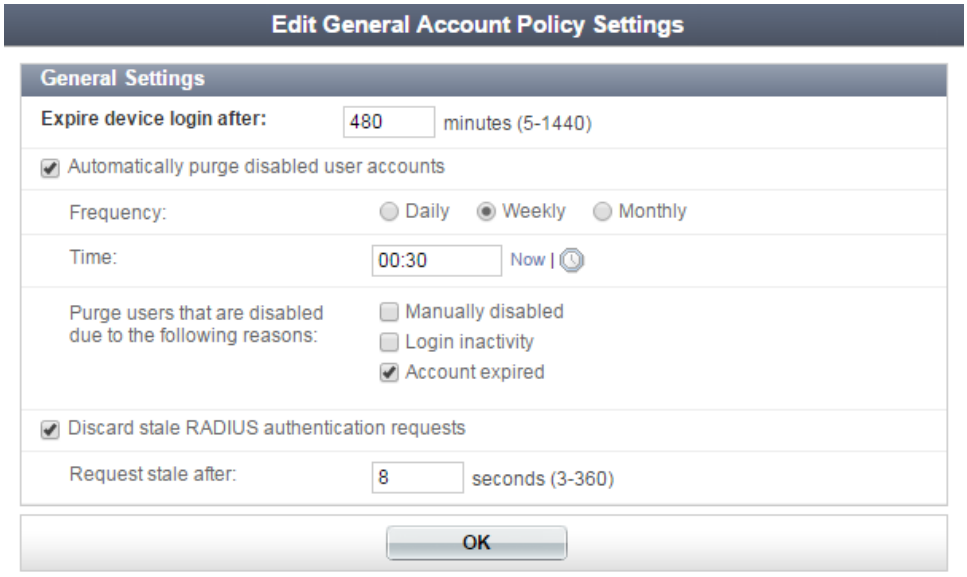
To configure machine authentication, see Clients on page 1.

User Account Policies

General policies for user accounts include lockout settings, password policies, and custom user fields.

General

To configure general account policy settings, go to *Authentication > User Account Policies > General*.



Configure the following settings:

Valid window	**Time-based:** Configure the length of time, plus or minus the current time, that a FortiToken code is deemed valid, from 1 to 60 minutes (default = 1 minute). **Event-based:** Configure the count, or number of times, that the FortiToken passcode is deemed valid, from 3 to 100 counts (default = 3 counts).
Sync window	**Time-based:** Configure the period of time in which the entry of an invalid token can trigger a synchronization, from 5 to 480 minutes (default = 60 minutes). **Event-based:** Configure the count, or number of times, that the entry of an invalid token can trigger a synchronization, from 5 to 100 counts (default = 100 counts). If the token is incorrect according to the FortiToken valid window, but exists in the sync window, synchronization will be initiated.
E-mail/SMS token timeout	Set a time after which a token code sent via email or SMS will be marked as expired, from 10 to 3600 seconds.
Expire device login after	Set a time after which a machine authenticated device will be automatically expired, from 5 to 1440 minutes (default = 480 minutes).
Automatically purge expired user accounts	Select to automatically purge expired user accounts. Select the frequency of the purge in the *Frequency* field: *Daily*, *Weekly*, or *Monthly*. Enter the time of the purge in the *Time* field, select *Now* to set the time to the current time, or select the clock icon to choose a time: *Now*, *Midnight*, *6 a.m.*, or *Noon*. Set the reason for purging disabled users: *Manually disabled*, *Login inactivity*, or *Account expired*.
Restrict web service access to a specific interface	Select to restrict web service access to a specific port, then select the port from the *Web service interface* drop-down list.
Discard stale RADIUS authentication requests	Select to set a time after which RADIUS authentication requests are discarded (default = 5 seconds).

Lockouts

For various security reasons, you may want to lock a user's account. For example, repeated unsuccessful attempts to log in might indicate an attempt at unauthorized access.

Information on locked out users can be viewed in the *Top User Lockouts* widget, see Top User Lockouts widget on page 1.

Currently locked out users can be viewed in *Monitor* > *Authentication* > *Inactive Users*, see Inactive users on page 1.

To configure the user lockout policy:

1. Go to *Authentication* > *User Account Policies* > *Lockouts*.
2. Configure the following settings, then select *OK* to apply any changes:

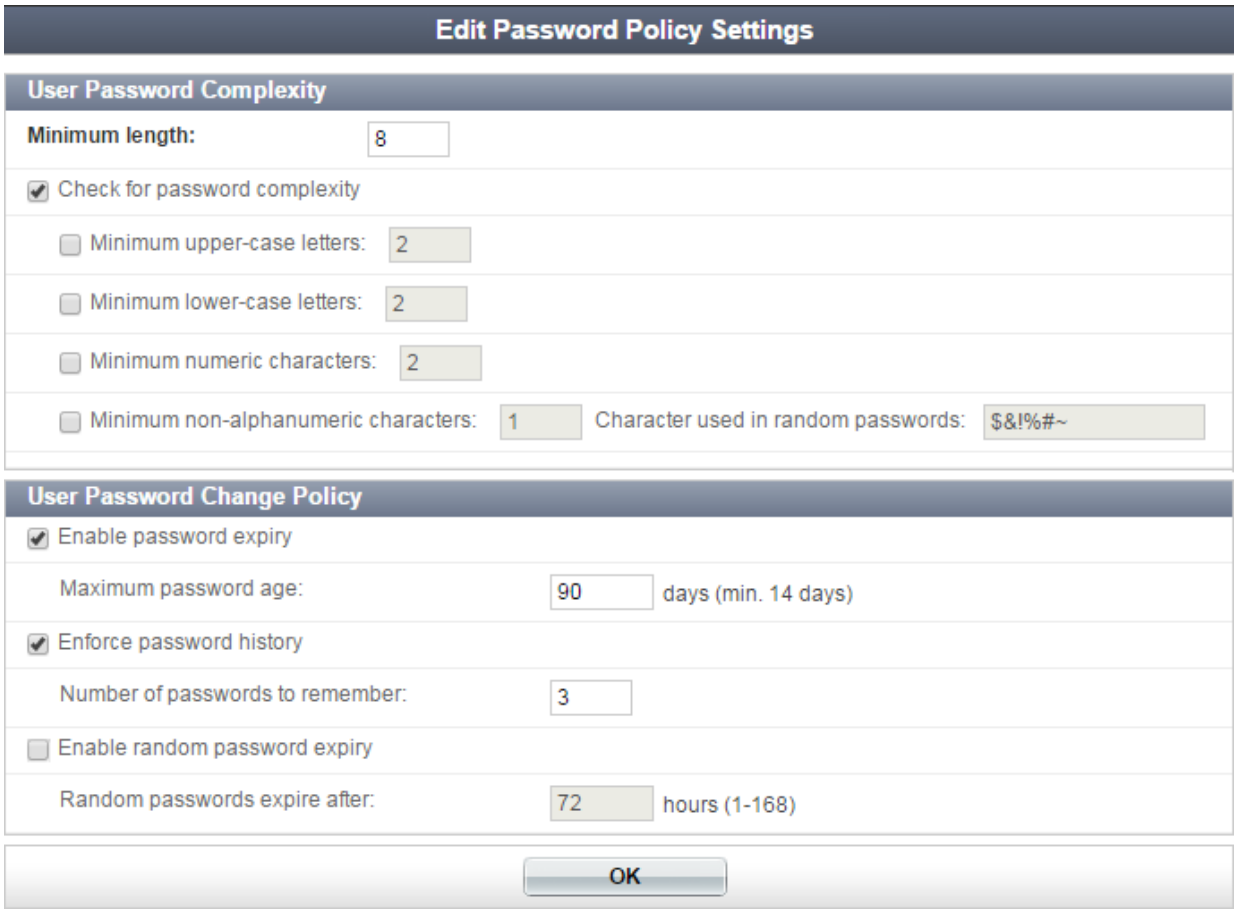
Enable user account lockout policy	Enable user account lockout for failed login attempts and enter the maximum number of allowed failed attempts in the *Max. failed login attempts* field.
Specify lockout period	Select to specify the length of the lockout period, from 60 to 86400 seconds. After the lockout period expires, the *Max. failed login attempts* number applies again. When disabled, locked out users will be permanently disabled until an administrator manually re-enables them.
Enable inactive user lockout	Select to enable disabling a user account if there is no login activity for a given number of days. In the *Lock out inactive users after* field, enter the number of days, from 1 to 1825, after which a user is locked out.

Passwords

You can enforce a minimum length and complexity for user passwords, and can force users to change their passwords periodically.

For information on setting a user's password, and password recovery options, see Editing a user on page 1.

Go to *Authentication* > *User Account Policies* > *Passwords* to configure password policy settings.



To set password complexity requirements:

1. In *User Password Complexity*, enter the minimum password length in the *Minimum length* field.

The default minimum length is 0, which means that there is no minimum length but the password cannot be empty.

1. Optionally, select *Check for password complexity* and then configure the following password requirements as needed:
   - Minimum upper-case letters
   - Minimum lower-case letters
   - Minimum numeric characters
   - Minimum non-alphanumeric characters
     You can configure which non-alphanumerical characters may be used in random password generation by entering them in the *Characters used in random passwords* field.
2. Select *OK* to apply the password length and complexity settings.

To set a password change policy:

1. In *User Password Change Policy*, optionally select *Enable password expiry*, then set the maximum allowed password age in the *Maximum password age* field.

   The default maximum password age is 90 days. The minimum value allowed is 14 days.

2. Optionally, select *Enforce password history* to prevent users from creating a new password that is the same as their current password or recently used passwords.

   Then, enter the number of password to remember in the *Number of passwords to remember* field. New passwords must not match any of the remembered passwords. For example, if three passwords are remembered, users cannot reuse any of their three previous passwords.

3. Optionally, select *Enable random password expiry* to force randomly generated passwords to expire. Then, enter the length of time after which a randomly generated password will expire in the *Random passwords expire after* field.

   The default randomly generated password expiry age is 72 hours. The value can be set from 1 to 168 hours.

4. Select *OK* to apply the password change policy settings.

Custom User Fields

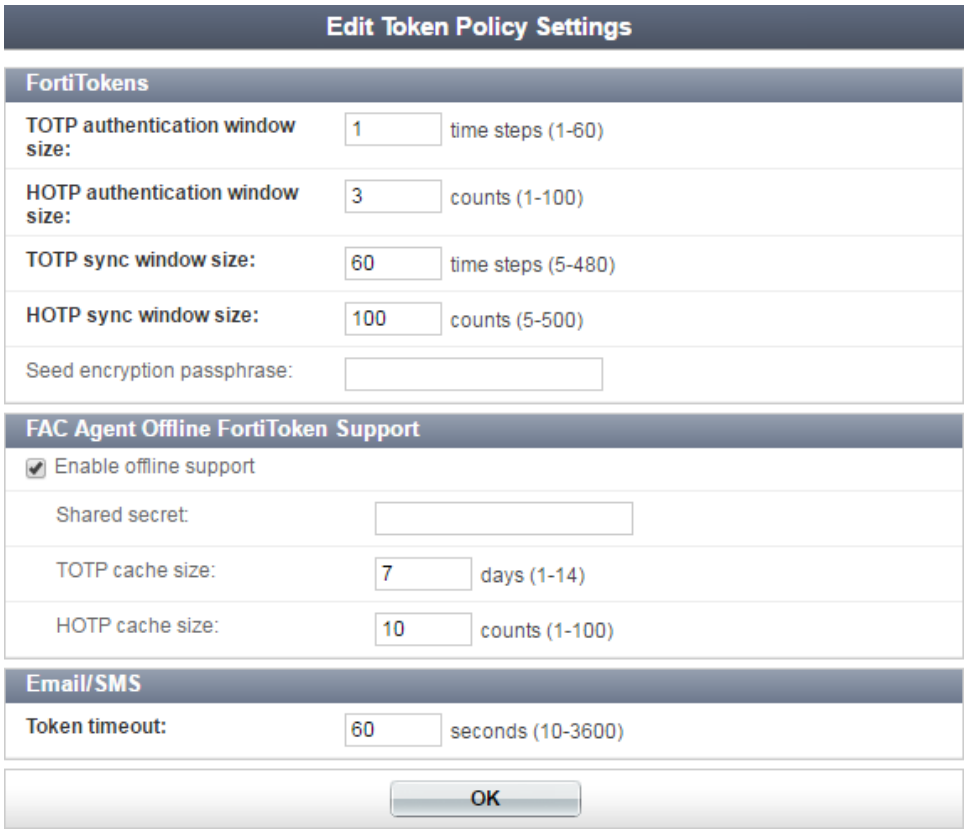
Custom fields can be created to be included in the user information of local users. See Local users on page 1 for information about creating and managing local users.

To edit custom fields, go to *Authentication* > *User Account Policies* > *Custom User Fields*. A maximum of three custom fields can be added.

Tokens

As of FortiAuthenticator 4.2, all FortiToken settings have been moved here to be configured and controlled separately from the general user account policy settings. Additionally, now you can configure the FortiAuthenticator to allow the Windows Agent to cache future tokens for users when they're offline by using the *Enable offline support* setting.

To configure token policy settings, go to *Authentication* > *User Account Policies* > *Tokens*.



Configure the following settings:

FortiTokens		
	TOTP authentication window size	Configure the length of time, plus or minus the current time, that a FortiToken code is deemed valid, from 1 - 60 minutes (default is 1 minute).
	HOTP authentication window size	Configure the count, or number of times, that the FortiToken passcode is deemed valid, from 1 - 100 counts (default is 3 counts).
	TOTP sync window size	Configure the period of time in which the entry of an invalid token can trigger a synchronization, from 5 - 480 minutes (default is 60 minutes). If the token is incorrect according to the FortiToken valid window, but exists in the sync window, synchronization will be initiated.
	HOTP sync window size	Configure the count, or number of times, that the entry of an invalid token can trigger a synchronization, from 5 - 500 counts (default is 100 counts). If the token is incorrect according to the FortiToken valid window, but exists in the sync window, synchronization will be initiated.

	Seed encryption passphrase	Passphrase to derive a seed encryption key from, for seed returned when provisioning a FortiToken Mobile via web service (REST API).
FAC Agent Offline FortiToken Support		
	Enable offline support	Enable this option to set the following: **Shared secret:** Set the shared secret used in offline support. **TOTP cache size:** Period of time after last login to pre-cache offline TOTP tokens, from 1 - 14 days (default is 7 days). **HOTP cache size:** Period of time after last login to pre-cache offline HOTP tokens, from 1 - 100 counts (default is 10 counts).
Email/SMS		
	Token timeout	Set a time after which a token code sent via email or SMS will be marked as expired, from 10 - 3600 seconds (default is 60 seconds).

User Management

FortiAuthenticator's user database has the benefit of being able to associate extensive information with each user, as you would expect of RADIUS and LDAP servers. This information includes whether the user is an administrator, uses RADIUS authentication, or uses two-factor authentication, and includes personal information such as full name, address, password recovery options, and the groups that the user belongs to.

The RADIUS server on the FortiAuthenticator unit is configured using default settings. For a user to authenticate using RADIUS, the option *Allow RADIUS Authentication* must be selected for that user's entry, and the FortiGate unit must be added to the authentication client list. See RADIUS service on page 1.

This section includes the following subsections:

Administrators

Administrator accounts on FortiAuthenticator are standard user accounts that are flagged as administrators. Both local users and remote LDAP users can be administrators.

Once flagged as an administrator, a user account's administrator privileges can be set to either full access or customized to select their administrator rights for different parts of the FortiAuthenticator unit.

The subnets from which administrators are able to log in can be restricted by entering the IP addresses and netmasks of trusted management subnets.

There are log events for administrator configuration activities. Administrators can also be configured to authenticate to the local system using two-factor authentication.

An account marked as an administrator can be used for RADIUS authentication if *Allow RADIUS Authentication* is selected. See RADIUS service on page 1. These administrator accounts only support Password Authentication Protocol (PAP).

See Configuring a user as an administrator on page 67 for more information.

Local Users

Local user accounts can be created, imported, exported, edited, and deleted as needed. Expired local user accounts can be purged manually or automatically (see General on page 1).

To manage local user accounts, go to *Authentication* > *User Management* > *Local Users*.

The local user account list shows the following information:

Create New	Select to create a new user.
Import	Select to import local user accounts from a CSV file or FortiGate configuration file. If using a CSV file, it must have one record per line, with the following format: user name (30 characters max), first name (30 characters max), last name (30 characters max), email address (75 characters max), mobile number (25 characters max), password (optional, 128 characters max). If the optional password is left out of the import file, the user will be emailed temporary login credentials and requested to configure a new password. Note: Even if an optional field is empty, it still must be defined with a comma.
Export Users	Select to export the user account list to a CSV file.
Disabled Users	**Purge Disabled:** This offers the option to choose which type of disabled users to purge. All users matching the type(s) selection will be deleted. **Re-enable:** This allows the administrator to re-enable disabled accounts. Expired users accounts can only be re-enabled individually.
Edit	Select to edit the selected user account.

Delete	Select to delete the selected user account or accounts.
Search	Enter a search term in the search field, then select *Search* to search the user account list.
Username	The user accounts' usernames.
First name	The user accounts' first names, if included.
Last name	The user accounts' last names, if included.
Email address	The user accounts' email addresses, if included.
Admin	If the user account is set as an administrator, a green circle with a check mark is shown.
Status	If the user account is enabled, a green circle with a check mark is shown.
Token	The token that is assigned to that user account. Select the token name to edit the FortiToken, see FortiToken device maintenance on page 1.
Groups	The group or groups to which the user account belongs.
Authentication Method	The authentication method used for the user account.
Expiration	The date and time that the user account expires, if an expiration date and time have been set for the account.

Adding a user

When creating a user account, there are three ways to handle the password:

- The administrator assigns a password immediately and communicates it to the user.
- The FortiAuthenticator unit creates a random password and automatically emails it to the new user.
- No password is assigned because only token-based authentication will be used.

To add a new user:

1. In the local users list, select *Create New*. The *Create New User* window opens.
2. Enter the following information:

Username	Enter a username for the user.

Password creation	Select one of three options from the drop-down list: • *Specify a password*: Manually enter a password in the *Password* field, then reenter the password in the *Password confirmation* field. • *Set and e-mail a random password*: Enter an email address to which to send the password in the *E-mail address* field, then reenter the email address in the *Confirm e-mail address* field. • *No password, FortiToken authentication only*: After you select *OK*, you will need to associate a FortiToken device with this user.
Enable account expiration	Select to enable account expiration, either after a specific amount of time has elapsed, or on a specific date.
Expire after	Select when the account will expire, one of: • *Set length of time*: Enter the amount of time in hours, days, months, or years, until the account expires. • *Set an expire date*: Enter the date on which the account will expire, either by manually typing it in, or by selecting the calendar icon then selecting a date on the pop-up calendar.

3. Select *OK* to create the new user.

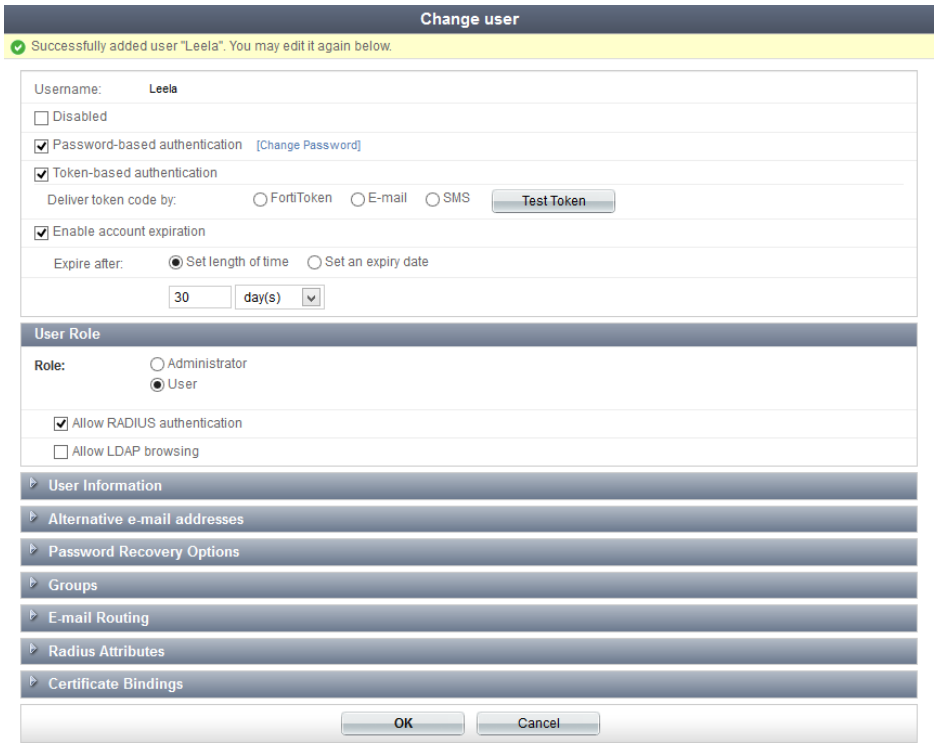
   You will be redirected to the *Change user* window to continue the user configuration.

   If the password creation method was set to No password, FortiToken authentication only you will be required to associate a FortiToken with the user before the user can be enabled. See FortiAuthenticator and FortiTokens on page 1.

Editing a user

User accounts can be edited at any time. When creating a new user, you will be immediately redirected to the *Change user* window to complete the user configuration.

To view the *Change user* window, go to the user account list, select the user you will be editing, and then select *Edit* from the toolbar. Conversely, selecting the username in the user list will also open the *Change user* window.



The following information can be viewed or configured:

Username	The user's username. This cannot be changed.
Disabled	Select to disable the user account.
Password-based authentication	Select to enable password based authentication. Select *Change Password* to open the Change password window, where you can change the user's password.
Token-based authentication	Select to enable FortiToken based authentication. See Configuring token based authentication on page 66.
Enable account expiration	Select to enable account expiration. See Enable account expiration on page 64.
User Role	Configure the user's role.
Role	Select *Administrator* or *User*. If setting a user as an administrator, see Configuring a user as an administrator on page 67.
Allow RADIUS authentication	Select to allow RADIUS authentication. This applies only to non-administrator users.
Allow LDAP browsing	Select to Allow LDAP browsing. This applies only to non-administrator users.

User Information	Enter user information, such as their address and phone number. See Adding user information on page 67.
Alternative e-mail addresses	Add alternate email addresses for the user.
Password Recovery Options	Configure password recovery options for the user. See Configuring password recovery options on page 68
Groups	Assign the user to one or more groups. See User groups on page 73.
E-mail Routing	Enter a mail host and routing address into their respective fields to configure email routing for the user.
Radius Attributes	Add RADIUS attributes. See RADIUS Attributes on page 76.
Certificate Bindings	Add, edit, or removed certificate bindings for the user account. See Configuring certificate bindings on page 69. Select the certificate name to view the certificate, or select the *Revoke Certificate* button to revoke the certificate.

Select *OK* when you have finished editing the user's information and settings.

Configuring token based authentication

Token-based authentication requires one of the following:

- a FortiToken device or mobile device with the FortiToken Mobile app installed,
- a device with either email or SMS capability.

If a FortiToken device or FortiToken Mobile app will be used, it must first be registered in *Authentication* > *User Management* > *FortiTokens*. See FortiTokens on page 75 for more information.

To configure an account for token-based authentication:

1. Go to the *Change user* window for the requisite user account.
2. Select *Token-based authentication* to view the token-based authentication options.
3. Do one of the following:
   - Select *FortiToken*, then select the FortiToken device serial number from the *FortiToken Hardware* or *FortiToken Mobile* drop-down lists, as appropriate.

     The device must be known to the FortiAuthenticator unit. See FortiToken devices and mobile apps on page 1.

     Optionally, select *Configure a temporary e-mail/SMS token* to receive a temporary token code via email or SMS.
   - Select *Email* and enter the user's email address in the *User Information* section.
   - Select *SMS* and enter the user's mobile number in the *User Information* section.
4. Select *Test Token* to validate the token passcode. The *Test Email Token* or *Test SMS Token* window opens (depending on your selection).

a. For email and SMS tokens, confirm that the contact information is correct, select *Next*, then enter the token code received via email or SMS.
b. Select *Back* to return to edit the contact information, select *Verify* to verify the token passcode, or select *Resend Code* if a new code is required.
c. For FortiToken, enter the token code in the *Token code* field, then select *Verify* to verify the token passcode.

5. Select *OK*.

By default, token-based authentication must be completed within 60 seconds after the token passcode is sent by email or SMS. To change this timeout, go to *Authentication* > *User Account Polices* > *General* and modify the *Email/SMS Token Timeout* field, see Lockouts on page 1.

Configuring a user as an administrator

See Administrators on page 62 for more information.

To set a user as an administrator:

1. Go to the *Change user* window for the requisite user account.
2. In the *User Role* section, select *Administrator* for the *Role*.
3. In the *Access* field, select *Full* to give the administrator fill administrative privileges, or select *Custom* to customize the administrator's permissions.

   If *Custom* is selected, find the permissions that the user will have in the *Available user permissions* list, and move them to the *Selected user permissions* list.
4. Optionally, select *Web service access* to allow the administrator to access the web services via a REST API or FortiAuthenticator Agent for Microsoft Windows.
5. Select *Restrict admin login from trusted management subnets only*, then enter the IP addresses and netmasks of trusted management subnets in the table, to restrict the subnets from which an administrator can log in.
6. Select *OK* to apply the changes to the user.

Adding user information

User information can be added in the *Change user* window. Some information can be required depending on how the user is configured. For example, is the user is using token-based authentication by SMS, then a mobile number and SMS gateway must be configured before the user can be enabled.

The following user information can be entered:

First name	*Last name*
Email address	*Phone number*
Mobile number	*SMS gateway*: select from the drop-down list. Select *Test SMS* to send a test message.
Street address	
City	*State/Province*
Country: Select from the drop-down list.	

Language: select a specific language from the drop-down list, or use the default language.

Organization: select an organization from the drop-down list. See Organizations on page 74.

Max. devices: Select either *Use global configuration*, or *Specify a custom number*.

User has: The number of device the user currently has.

Custom user fields: See Custom User Fields on page 1 for more information.

Configuring password recovery options

To replace a lost or forgotten password, the FortiAuthenticator unit can send the user a password recovery link by email or in a browser in response to a pre-arranged security question. The user then must set a new password.

To configure password recovery by email:

1. Go to the *Change user* window for the requisite user account.
2. Ensure that the user has an email address entered. See Adding user information on page 67.
3. In the *Password Recovery Options* section, Select *E-mail recovery*.
4. Optionally, select *Alternative e-mail addresses* and enter additional email addresses for this user.
   In the event of password recovery, an email message will be sent to all configured email addresses — both the user information email address and the alternative email addresses.
5. Select *OK* to apply the changes.

To configure password recovery by security question:

1. Go to the *Change user* window for the requisite user account.
2. In the *Password Recovery Options* section, select *Security question*, then select *Edit*. The *Setup a Security Question* dialog box opens.
3. Choose one of the questions in the list, or select *Write my own question* and enter a question in the *Custom question* field.
4. Enter the answer for the question in the *Answer* field.
5. Select *OK* to create the security question.
6. Select *OK* in the *Change user* window to apply your changes.

How the user can configure password recovery by security question:

1. Log in to the user account. The *View Profile* page opens.
2. Select *Edit Profile* at the top left of the page.
3. In the *Password Recovery Options* section, select *Security Question*, and select *Edit*.
4. Choose one of the questions in the list, or select *Write my own question* and enter a question in the *Custom question* field.
5. Enter the answer for your question.
6. Select *OK*.

How the user can configure password recovery by email:

1. Log in to the user account. The *View Profile* page opens.
2. Select *Edit Profile* at the top left of the page.
3. In the *Password Recovery Options* section, select *E-mail recovery*.
4. Optionally, select *Alternative e-mail addresses* and enter additional email addresses for this user.
5. Select *OK*.

How the user recovers from a lost password:

1. Browse to the IP address of the FortiAuthenticator.
   Security policies must be in place on the FortiGate unit to allow these sessions to be established.
2. At the login screen, select *Forgot my password*.
3. Select either *Username* or *Email* as your method of recovery.
4. Enter either your username or email address as selected in the previous step, and then select *Next*.
   This information is used to select the user account. If your information does not match a user account, password recovery cannot be completed.
5. Do one of the following:
   - If an email address was entered, check your email, open the email and select the password recovery link.
   - If a username was entered, answer the security question and then select *Next*.

   The recovery options available depend on the settings in the user account.
6. On the *Reset Password* page, enter and confirm a new password and then select *Next*.
   The user can now authenticate using the new password.

Configuring certificate bindings

To use a local certificate as part of authenticating a user, you need to:

- Create a user certificate for the user, see To create a new certificate on page 1.
- Create a binding to that certificate in the user's account.

To create a binding to a certificate in a user's account:

1. Go to the *Change user* window for the requisite user account.
2. Expand the *Certificate Bindings* section.
3. Select *Add Binding*. The *Create New Local User Certificate Binding* window opens.
4. Select either *Local CA* or *Trusted CA* and then select the applicable CA certificate from the drop-down list.
5. Enter the *Common Name* on the certificate. For example, if the certificate says `CN=rgreen` then enter `rgreen`.
6. Select *OK* to add the new binding.

Remote Users

Remote LDAP users must be imported into the FortiAuthenticator user database from LDAP servers, see LDAP on page 1. A maximum of five users can be imported.

A FortiToken device already allocated to a local account cannot be allocated to an LDAP user as well; it must be a different FortiToken device.

Remote RADIUS users can be created, migrated to LDAP users, edited, and deleted.

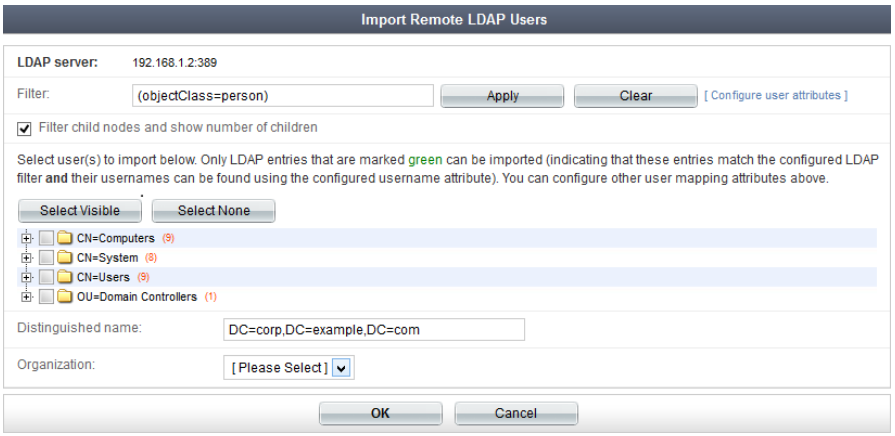
LDAP users

To import remote LDAP users:

1. Go to *Authentication* > *User Management* > *Remote Users*, ensure that *LDAP users* is selected, then select *Import*. The *Import Remote LDAP Users* screen open.
2. Select a remote LDAP server from the *Remote LDAP Server* drop-down list, then select *Import Users*.

An LDAP server must already be configured to select it in the drop-down list. See Remote authentication servers on page 1 for information on adding a remote LDAP server.

The *Import Remote LDAP Users* window opens in a new browser window.



3. Optionally, enter a *Filter* string to reduce the number of entries returned, and then select *Apply*, or select *Clear* to clear the filters.
4. The default configuration imports the attributes commonly associated with Microsoft Active Directory LDAP implementations. Select *Configure user attributes* to edit the remote LDAP user mapping attributes.

   Selecting the field, *FirstName* for example, presents a list of attributes which have been detected and can be selected. This list is not exhaustive and additional, non-displayed attributes may be available for import. Consult your LDAP administrator for a list of available attributes.
5. Select the entries you want to import.
6. Optionally, select an organization from the *Organization* drop-down to associated the imported users with a specific organization. See Organizations on page 74.
7. Select *OK*.

   The amount of time required to import the remote users will vary depending on the number of users being imported.

To add two-factor authentication to a remote LDAP user:

1. From the remote user list, select the user you are editing. The *Edit Remote LDAP User* window opens.
2. Select *Token-based authentication*, then follow the same steps as when editing a local user (Editing a user on page 64).
3. Configure the *User Role*, *User Information*, *Radius Attributes*, and *Certificate Bindings* for the user as needed.
4. Select *OK* to apply the changes.

RADIUS users

To view remote RADIUS users, go to *Authentication* > *User Management* > *Remote Users* and select *RADIUS users* in the toolbar. See RADIUS on page 1 for more information about remote RADIUS servers.

The following options are available:

Create New	Select to create a new remote RADIUS user.
Delete	Select to delete the selected user or users.
Edit	Select to edit the selected user.
Migrate	Select to migrate the selected user or users. See To migrate RADIUS users to LDAP users: on page 72.
Token-based Auth	Select to enforce or bypass token-based authentication for the selected user or users.
Search	Search the remote RADIUS user list.
Username	The remote user's name.
Remote RADIUS server	The remote RADIUS server or which the user resides.
Token	The FortiToken used by the user, if applicable.
Enforce token-based authentication	Whether or not token-based authentication is enforced.

To create a new remote RADIUS user:

1. From the remote user list, select *RADIUS users*, then select *Create New*. The *Create New Remote RADIUS User* window opens.
2. Enter the following information:

Remote RADIUS	Select the remote RADIUS server on which the user will be created from the drop-down list. For more information on remote RADIUS servers, see RADIUS on page 1.
Username	Enter a username.

Enforce token-based authentication if configured below	Select to enforce the token-based authentication, if you are configuring token-based authentication.
Token-based authentication	Select to configure token-based authentication.
Deliver token code by	Select the method by which token code will be delivered. One of: • *FortiToken*: select the FortiToken device serial number from the *FortiToken Hardware* or *FortiToken Mobile* drop-down lists, as appropriate. 1. The device must be known to the FortiAuthenticator unit. See FortiToken devices and mobile apps on page 1. 2. Optionally, select *Configure a temporary e-mail/SMS token* to receive a temporary token code via email or SMS. • *Email*: enter the user's email address in the *User Information* section. • *SMS*: enter the user's mobile number in the *User Information* section.
User Information	**Enter user information as needed. The following options are available:** • *Email address* • *Mobile number* and *SMS gateway* • *Language* • *Organization* - see Organizations on page 74.

3. Select *OK* to create the new remote RADIUS user.

To migrate RADIUS users to LDAP users:

1. From the remote RADIUS users list (see Learned RADIUS users on page 1), select the user or users you need to migrate, then select *Migrate* from the toolbar. The *Migrate RADIUS Users to LDAP Users* window opens.
2. Select a LDAP server from the drop down list to which the selected RADIUS user or users will be located, then select *Next*.
3. Enter the distinguished names for the users that are being migrated, or browse the LDAP tree (see Directory tree overview on page 1) to find the users.
4. Select *Migrate* to migrate the user or users.

Remote user sync rules

Synchronization rules can be created to control how and when remote users are synchronized. To view a list of the remote user synchronization rules, go to *Authentication* > *User Management* > *Remote User Sync Rules*.

To create a new remote user synchronization rule:

1. From the *Remote User Sync Rules* page, select *Create New*. The *Create New Remote User Synchronization Rule* windows opens.

2. Configure the following settings:

Name	Enter a name for the synchronization rule.
Remote LDAP	Select a remote LDAP server from the drop-down list. To configure a remote LDAP server, see Remote authentication servers on page 1.
Sync every	Select the amount of time between synchronizations.
LDAP filter	Optionally, enter an LDAP filter. Select *Test Filter* to test that the filter functions as expected.
Token-based authentication sync priorities	Select the required authentication synchronization priorities. Drag the priorities up and down in the list change the priority order.
Sync as	Select to synchronize as a remote user or as a local user. Selecting either option will open a pop-up dialog box displaying the user fields that will be synchronized for that selection.
Group to associate users with	Optionally, select a group from the drop-down list with which to associate the users with, or select Create New to create a new user group. See User groups on page 73.
Organization	Optionally, select an organization from the drop-down list with which to associate the users with, or select *Create New* to create a new organization. See Organizations on page 74.
LDAP User Mapping Attributes	Optionally, edit the remote LDAP user mapping attributes.
Preview Mapping	Select to preview the LDAP user sync mappings in a new window.
Show Sync Fields	Select to view the user fields that will be synchronized.

3. Select *OK* to create the new synchronization rule.

User groups

Users can be assigned to groups during user account configuration (see Editing a user on page 64), or by editing the groups to add users to it.

To view the user groups list, go to *Authentication* > *User Management* > *User Groups*.

To create a new user group:

1. Go to *Authentication* > *User Management* > *User Groups* and select *Create New*. The *Create New User Group* window opens.
2. Enter the following information:

Name	Enter a name for the group.
Type	Select the type of group, *Local*, *Remote LDAP*, or *Remote RADIUS*.

Users	Select users from the Available users box and move them to the Selected users box to add them to the group. This option is only available if Type is Local.
User retrieval	Determine group membership by selecting either *Specify an LDAP filter* or *Set a list of imported remote users*. This option is only available if *Type* is *Remote LDAP*.
Remote LDAP	Select a remote LDAP server from the drop-down list. At least one remote LDAP server must already be configured, see Remote authentication servers on page 1. This option is only available if *Type* is *Remote LDAP*.
Remote RADIUS	Select a remote RADIUS server from the drop-down list. At least one remote RADIUS server must already be configured, see Remote authentication servers on page 1. This option is only available if *Type* is *Remote RADIUS*.
LDAP filter	Enter an *LDAP filter*. Optionally, select *Test filter* to ensure that the filter works as expected. This option is only available if *Type* is *Remote LDAP* and *User retrieval* is set to *Specify an LDAP filter*.
LDAP users	Select remote LDAP users from the *Available LDAP users* box and move them to the *Selected LDAP users* box to add them to the remote group. This option is only available if *Type* is *Remote LDAP* and *User retrieval* is set to *Set a list of imported remote users*.
RADIUS users	Select remote RADIUS users from the *Available RADIUS users* box and move them to the *Selected RADIUS users* box to add them to the remote group. This option is only available if *Type* is *Remote RADIUS*.

3. Optionally, you may enable *Allow token self-provisioning*. For more details, see Token self-provisioning on page 1.
4. Select *OK* to create the new group.

To edit a user group:

1. In the user group list, select the group that you need to edit.
2. Edit the settings as required. The settings are the same as when creating a new group.
3. Select *OK* to apply your changes.

Organizations

Organizations include a name and logo. An organization can be associated with local and remote users.

When a user provisions FortiToken Mobile on their device, the organization name and logo are automatically pushed to the device, allowing the FortiToken Mobile App's user interface to be rebranded.

Organizations can be created, edited, and deleted as needed. Organization are applied to users from the various user management pages. See Local Users on page 62, Remote Users on page 69, and Remote user sync rules on page 72.

To manage organizations, go to *Authentication* > *User Management* > *Organizations*.

To create a new organization:

1. From the organization list, select *Create New* to open the *Create New Organization* window.
2. Enter a name for the organization in the *Name* field.
3. Optionally, select *Browse...* to locate the logo image for the organization on your computer.

The image can be a maximum of 320x320 pixels, and must be 24-bit, and in the .PNG format.

4. Select *OK* to create the new organization.

FortiTokens

Go to *Authentication* > *User Management* > *FortiTokens* to view a list of configured FortiTokens. From here, FortiTokens can be added, imported, exported, edited, deleted, and activated. For more information, see FortiToken devices and mobile apps on page 1.

The following information is shown:

Create New	Create a new FortiToken, see To add FortiTokens manually: on page 1.
Import	Import a list of FortiTokens, see To import FortiTokens from a CSV file: on page 1 and To import FortiTokens from a FortiGate unit: on page 1.
Export	Export the FortiToken list, see To export FortiTokens: on page 1.
Delete	Delete the selected FortiToken or FortiTokens.
Edit	Edit the selected FortiToken or FortiTokens.
Activate	Activate the selected FortiToken or FortiTokens.
Search	Enter a search term in the search field, then select *Search* to search the FortiToken list.
Serial number	The FortiToken's serial number.
Token type	The FortiToken type, either *FortiToken Hardware* or *FortiToken Mobile*.
Status	Whether or not the FortiToken is activated.
Comment	Comments about the token.

User	The user to whom the FortiToken applies.
Size	The size of the token.
Drift	The time difference between the FortiAuthenticator and the FortiToken. For information on removing the drift, see FortiToken drift adjustment on page 1.
Timestep	The FortiToken timestep.
FTM License	The FTM license applied to the FortiToken.

MAC Auth Bypass

Non-802.1X compliant devices can be identified and accepted onto the network using MAC address authentication. See Non-compliant devices on page 1 for more information.

RADIUS Attributes

Some services can receive information about an authenticated user through RADIUS vendor-specific attributes. FortiAuthenticator user groups and user accounts can include RADIUS attributes for Fortinet and other vendors.

Attributes in user accounts can specify user-related information. For example, the *Default* attribute *Framed-IP-Address* specifies the VPN tunnel IP address to be sent to the user by the Fortinet SSL VPN.

Attributes in user groups can specify more general information, applicable to the whole group. For example, specifying third-party vendor attributes to a switch could enable administrative level login to all members of the *Network_Admins* group, or authorize the user to the correct privilege level on the system.

To add RADIUS attributes to a user or group:

1. Go to *Authentication* > *User Management* > *Local Users* and select a user account to edit, or go to *Authentication* > *User Management* > *User Groups* and select a group to edit.
2. In the *RADIUS Attributes* section, select *Add Attribute*. The *Create New User Group RADIUS Attribute* or *Create New User RADIUS Attribute* window opens.
3. Select the appropriate *Vendor* and *Attribute ID*, then enter the attribute's value in the *Value* field.
4. Select *OK* to add the new attribute to the user or group.
5. Repeat the above steps to add additional attributes as needed.

FortiToken devices and mobile apps

A FortiToken device is a disconnected one-time password (OTP) generator. It is a small physical device with a button that when pressed displays a six digit token passcode. FortiToken Mobile is an application for mobile devices that performs the same one-time password function as a FortiToken device.

Each FortiAuthenticator unit or virtual machine (VM) is supplied with two trial FortiToken Mobile tokens. To obtain the free FortiToken Mobile tokens (if they have not been created dynamically on install), select Get FortiToken Mobile trial tokens when adding a token.
This may be required if, for example, you are upgrading an unlicensed FortiAuthenticator unit to a licensed one, as the old tokens associated with the unlicensed serial number will not be compatible with the new, licensed serial number. The tokens will still work, but they are not able to be reassigned to a new user. In this case, you must delete the old tokens, and then generate new ones.

If using a token passcode that is time-based, it is imperative that the FortiAuthenticator unit clock is accurate. If possible, configure the system time to be synchronized with an NTP server.

To perform token-based authentication, the user must enter the token passcode. If the user's username and password are also required, this is called two-factor authentication. The displayed code changes every 60 seconds on a FortiToken device, and can be changed every 30 seconds on FortiToken Mobile.

FortiAuthenticator supports FortiToken OTP push notifications, or FTMv4 push notifications. Using FTMv4, when required to authenticate themselves, FortiToken Mobile users do not have to look-up a code in FortiToken and enter the code into their browser. Instead FortiToken Mobile is queried and the user just responds to accept the connection and the session is authenticated and access is allowed.

The FortiToken device has a small hole in one end. This is intended for a lanyard to be inserted so the device can be worn around the neck, or easily stored with other electronic devices. When not in use, the LCD screen is shut down to extend the battery life.

Do not put the FortiToken device on a key ring as the metal ring and other metal objects can damage it. The FortiToken is an electronic device like a cell phone and should be treated with similar care.

See FortiTokens on page 1 for more information.

FortiAuthenticator and FortiTokens

With FortiOS, FortiToken identifiers must be entered to the FortiGate unit, which then contacts FortiGuard servers to verify the information before activating them.

FortiAuthenticator acts as a repository for all FortiToken devices used on your network. It is a single point of registration and synchronization for easier installation and maintenance.

To register FortiTokens, you must have a valid FortiGuard connection. Otherwise, any FortiTokens you enter will remain in Inactive status. After the FortiTokens are registered, the connection to FortiGuard is no longer essential.
If a token authentication fails, check that the system time on the FortiAuthenticator unit is correct and then re-synchronize the FortiToken.

To add FortiTokens manually:

1. Go to *Authentication* > *User Management* > *FortiTokens* and select *Create New*. The *Create New FortiToken* window opens.
2. Select the *Token Type*, either *FortiToken Hardware* or *FortiToken Mobile*.
3. If *FortiToken Hardware* is selected as the *Token Type*, enter one or more token serial numbers in the *Serial numbers* field.

   You can also import multiple tokens by selecting *Import Multiple*, or by selecting *Add all FortiTokens from the same Purchase Order* then entering a single token's serial number; all tokens associated with that purchase order will then be imported.
4. If *FortiToken Mobile* is selected as the *Token Type*, enter the activation codes in the *Activation codes* field, or select *Get FortiToken Mobile free trial tokens* to use temporary tokens.
5. Select *OK* to add the FortiToken or FortiTokens.

To import FortiTokens from a CSV file:

1. From the FortiToken list, select *Import*. The *Import FortiTokens* window opens.
2. Do one of the following:
   - Select *Serial number file* to load a CSV file that contains token serial numbers for the tokens. (FortiToken devices have a barcode on them that can help you read serial numbers to create the import file.)
   - Select *Seed file* to load a CSV file that contains the token serial numbers, encrypted seeds, and IV values. (FortiToken devices have a barcode on them that can help you read serial numbers to create the import file.)
3. Select *Browse...*, find the configuration file, and select *Open*.
4. Select *OK* to import the FortiTokens.

To import FortiTokens from a FortiGate unit:

1. Export the FortiGate unit configuration to a file.
2. From the FortiToken list, select *Import*.
3. Select *FortiGate Configuration file*.
4. In the *Data to import* field, select *Import FortiToken Hardware only*, *Import FortiToken Hardware and only their associated users*, or Import all *FortiToken Hardware and users*.
5. Select *Browse...*, find the configuration file, then select *Open*.
6. If the file is encrypted, enter the password in the *Password* field.
7. Select *OK* to import the FortiTokens.

To export FortiTokens:

1. From the FortiToken list, select *Export FTK Hardware*.
2. Save the file to your computer.

Monitoring FortiTokens

To monitor the total number of FortiToken devices registered on the FortiAuthenticator unit, as well as the number of disabled FortiTokens, go to *System* > *Dashboard* > *Status* and view the *User Inventory* widget (see User Inventory widget on page 1).

You can also view the list of FortiTokens, their status, if their clocks are drifting, and which user they are assigned to from the FortiToken list found at *Authentication* > *User Management* > *FortiTokens*, see FortiTokens on page 1.

FortiToken device maintenance

Go to *Authentication* > *User Management* > *FortiTokens*, then select the FortiToken on which you need to perform maintenance and select *Edit*. The following actions can be performed:

- Comments can be added for FortiToken.
- The device can be locked if it has been reported lost or stolen.
  A reason for locking the device must be entered, and a temporary SMS token can be provided.
- The device can be unlocked if it is recovered.
- The device can be synchronized.
  Synchronize the FortiAuthenticator and the FortiToken device when the device clock has drifted. This ensures that the device provides the token code that the FortiAuthenticator unit expects, as the codes are time-based. Fortinet recommends synchronizing all new FortiTokens.
- The device history can be viewed, showing all commands applied to this FortiToken.

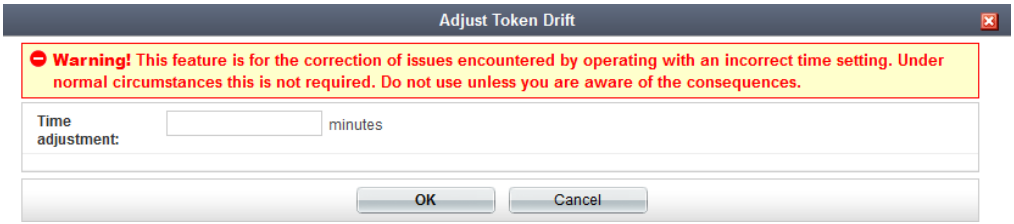
FortiToken drift adjustment

When the FortiAuthenticator unit and FortiTokens have been initialized prior to setting an NTP server, the time difference can be too large to correct with the synchronize function, forcing all tokens to resynchronize. To avoid this, selected tokens can be manually drift shifted.

The following procedure is intended to be used only in special cases where some FortiTokens are severely out-of-sync, for example, when a token is switched from manual configuration to NTP control. Under normal circumstances, this is not required.
Only activated FortiTokens can be adjusted.

To perform time drift adjustment on a FortiToken:

1. In a browser, go to `https://<FortiAuthenticator IP Address> /admin/fac_auth/fortitokendrift/`.
2. Select the FortiToken to adjust, then select *Adjust Drift*. The *Adjust Token Drift* window opens.



3. Enter the required *Time adjustment* in minutes.
   Include a minus sign for a negative value, but don't use a plus sign for a positive value.
4. Select *OK* to adjust the token drift.

Self-service portal

The self-service portal provides options for configuring general self-service portal options, access control settings, self-registration options, replacement messages, and device self-enrollment settings.

General

To configure general self-service portal settings, go to *Authentication* > *Self-service Portal* > *General*.

The following settings can be configured:

Default portal language	Select a default portal language from the drop-down list.
Add a Language Pack	Select to add a language pack. Several languages are included by default. A translation pack can be obtained from Fortinet support if you need to translate to your local language.
Site name	Enter a name that is used when referring to this site. If left blank, the default name will be the site DNS domain name or IP address.
E-mail Signature	Add a signature to be appended to the end of outgoing email messages.
Allow users to change their password	Select to allow users (local or remote or both) to change their password in the self-service portal.
Local users	Allow local users to change their password.
Remote users	Allow remote users to change their password (this includes non-imported remote LDAP users).

Access control

To configure self-service portal access settings, go to *Authentication* > *Self-service Portal* > *Access Control*.

The following settings can be configured:

Username input format	Select the input format for the username, one of: *username@realm*, *realm\username*, *realm/username*. The realm name is optional when authentication against the default realm.

Realms	Add realms to which the user will be associated. See Realms on page 1. • Select a realm from the drop-down list in the *Realm* column. • Select whether or not to allow local users to override remote users for the selected realm. • Edit the group filter as needed. That is, filter users based on the groups they are in. • If necessary, add more realms to the list. • Select the realm that will be the default realm for this client.

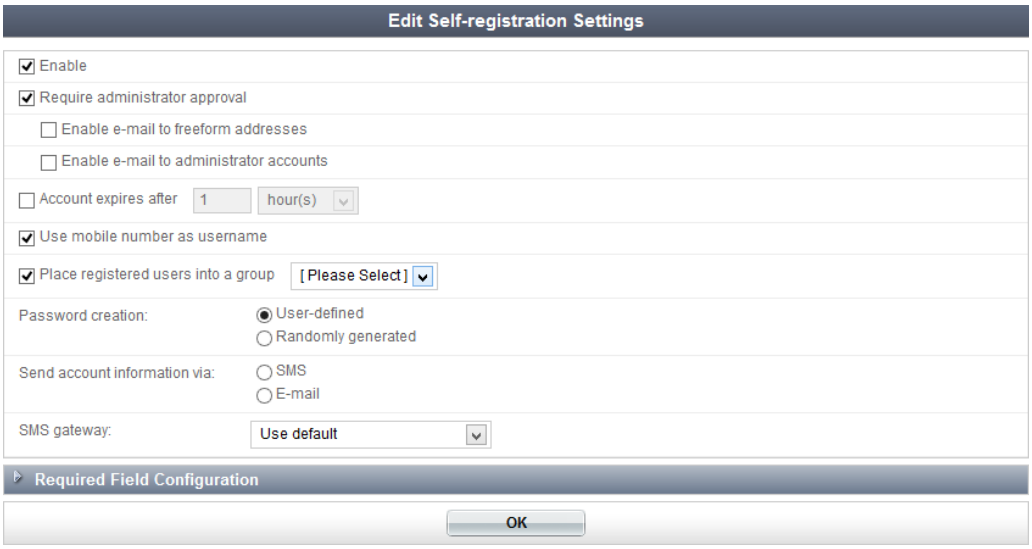
Self-registration

When self-registration is enabled, users can request registration through the FortiAuthenticator login page. Self-registration can be configured so that a user request is emailed to the device administrator for approval.

When the account is ready for use, the user receives an email or SMS message with their account information.

To enable self-registration:

1. Go to *Authentication* > *Self-service Portal* > *Self-registration*.



2. Select *Enable* to enable self-registration.
3. Optionally, configure the following settings:

Require administrator approval	Select to require that an administrator approves the user.
Enable e-mail to freeform addresses	Select to send self-registration requests to the email addresses entered in the *Administrator e-mail addresses* field.

Enable e-mail to administrator accounts	Select to send self-registration requests to specific administrators. Select the required administrators from the *Available administrators* box and move them to the *Chosen administrators* box.
Account expires after	Select to specify how long until self-generated accounts will be deleted after they are generated.
Use mobile number as username	If enabled, after a successful registration, the user's password will be sent to them via SMS to confirm their identity.
Place registered users into a group	Select a group into which self-registered users will be placed from the drop-down list.
Password creation	**Select how a password is created, either *User-defined* or *Randomly generated*.**
Send account information via	**Choose how to send account information to the user, either *SMS*, *E-mail*, or *Display on browser page*. The *Display on browser page* option is only available if administrator approval is not required.**
SMS gateway	**Select an SMS gateway from the drop-down list. See SMS gateways on page 1 for more information.**
Required Field Configuration	**Select the fields that the user is required to populate when self-registering. Options include: *First name*, *Last name*, *E-mail*, *address*, *Address*, *City*, *State/Province*, *Country*, *Phone number*, *Mobile number*, *Custom field 1*, *Custom field 2*, and *Custom field 3*. For information about custom fields, see Custom user fields on page 1.**

4. Select *OK* to apply your changes.

To approve a self-registration request:

1. Select the link in the *Approval Required for...* email message to open the *New User Approval* page in your web browser.
2. Review the information and select either *Approve* or *Deny*, as appropriate.

   Approval is required only if *Require administrator approval* is enabled in the self-registration settings.

   If the request is approved, the FortiAuthenticator unit sends the user an email or SMS message stating that the account has been activated.

How a user requests registration

A user can request registration, or self-register, from the FortiAuthenticator login screen.

To request registration:

1. Browse to the IP address of the FortiAuthenticator unit.

   Security policies must be in place on the FortiGate unit to allow these sessions to be established.

2. Select *Register* to open the user registration page.
3. Fill in all the required fields and, optionally, fill in the *Additional Information* fields
4. Select *OK* to request registration.

   If administrator approval is not required and *Display on browser page* is enabled, the account details are immediately displayed to the user.

Token self-provisioning

User token self-provisioning allows users to set up their own FortiTokens without direct intervention of an administrator.

To configure token self-provisioning settings, go to *Authentication* > *Self-service Portal* > *Token self-provisioning*.

The following settings can be configured:

Token Self-registration	
Allow FortiToken Hardware self-provisioning	Enable this option if you want to allow users to self-provision their own FortiToken Hardware tokens.
Allow FortiToken Mobile self-provisioning	Enable this option if you want to allow mobile users to self-provision their FortiToken.
Allow user to request a token from Administrator at this email address	Enable this option if you want to allow users to request a new token using an email address.

Token Self-revocation	
Allow users to report a lost token to the Administrator at this email address	Enable this option if you want to allow users to report a lost token.
Allow users to temporarily use SMS token authentication if a mobile number was pre-configured	Enable this option if you want to allow users to switch to temporary SMS based authentication. The administrator will also be notified.
Allow users to temporarily use email token authentication if an email was pre-configured	Enable this option if you want to allow users to switch to temporary email based authentication. The administrator will also be notified.
Allow users to re-provision their FortiToken Mobile	Enable this option if you want to allow mobile users to re-provision their token.

How a user registers a token

If enabled, a user can self-register a token from the user portal screen.

To self-register:

1. Browse to the IP address of the user portal and log in.
2. Go to *My Account* > *User* > *Register Token* to open the token registration options.
3. Fill in all the required fields.
   Only options that the administrator has configured under the Token Self-registration options will be available.
4. Select *OK* to register token.
   If a token is already assigned to the user, the token registration page will display the token along with its serial number.

How a user reports a lost token

A user can report a lost token (mobile or physical) from the user portal screen.

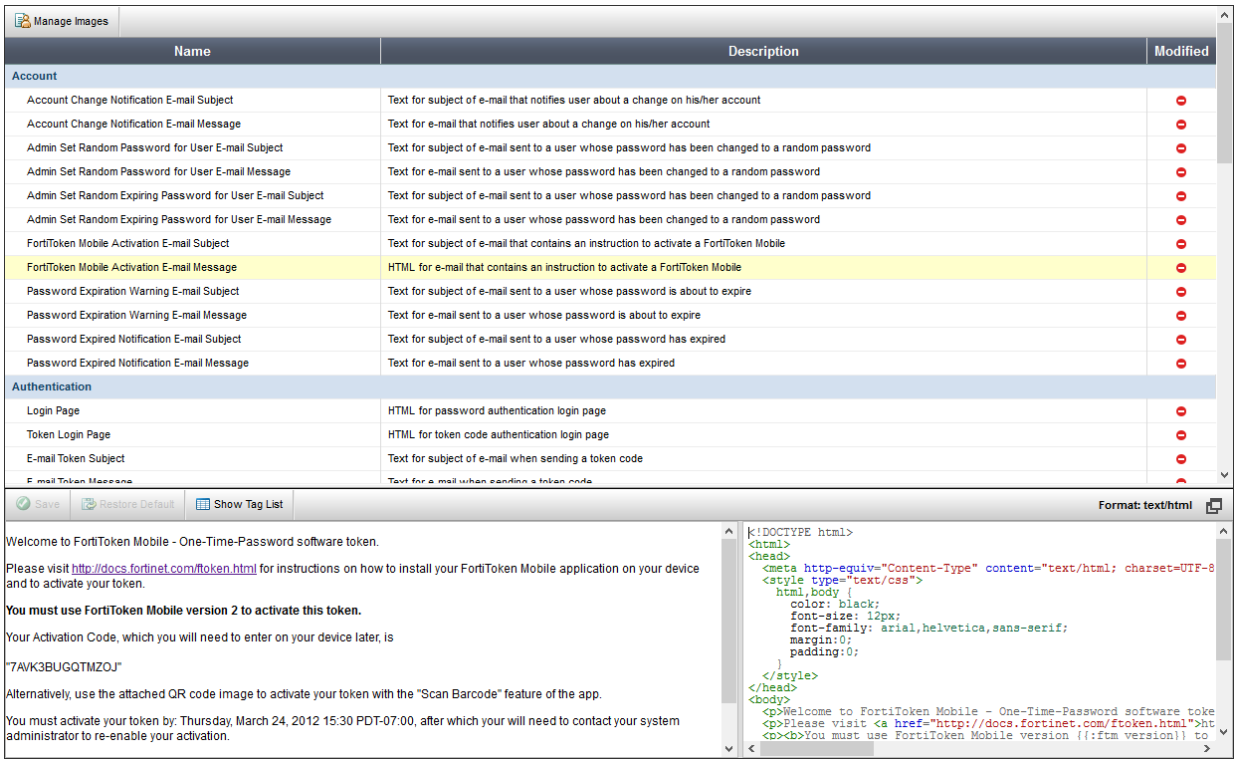
To report lost token:

1. Browse to the IP address of the user portal.
2. Select *I lost my token*.
   The user will be directed to a page warning them that their account will be locked and the administrator will be notified. Select *OK* to continue.
3. Select the preferred option.
   Only options that the administrator has configured under the Token Self-revocation options will be available.
4. Select *OK* to continue.

Replacement Messages

The replacement messages list enables you to view and customize replacement messages, and manage images.

Go to *Authentication* > *Self-service Portal* > *Replacement Messages* to view the replacement message list.



The replacement messages are split into five categories: *Account*, *Authentication*, *Device Certificate Enrollment*, *Password Reset*, and *User Registration*.

Selecting a specific message will display the text and HTML or plain text of the message in the lower half of the content pane.

Selecting *Show Tag List* will display a table of the tags used for that message atop the message's HTML or plain text box.

To edit a replacement message:

1. Select a message in the replacement message list.
2. Edit the plain text or HTML code in the lower right pane, or select the open in new window icon to edit the message in a new browser window.
3. When you are finished editing the message, select *Save* to save your changes.
4. If you have made an error when editing the message, select *Restore Default* to restore the message to its default value.

Manage Images

Images can be managed by selecting *Manage Images* in the *Replacement Messages* window. Images can also be added, deleted, and edited.

To add an image:

1. In the manage images screen, select *Create New* to open the *Create New Image* window.
2. Enter a name for the image in the *Name* field.
3. Select *Browse...*, find the GIF, JPEG, or PNG image file that you are adding, and then select *Open*.

The maximum image size is 65kB.

4. Select *OK* to add the image.

To delete an image:

1. In the manage images screen, select an image, then select *Delete*.
2. Select *Yes, I'm sure* in the confirmation window to delete the image.

To edit an image:

In the manage images screen, select an image, then select *Edit*.

1. In the *Edit Image* window, edit the image name and file as required.
2. Select *OK* to apply your changes.

Since the release of FortiAuthenticator 4.2, three new Authentication replacement messages have been added: *Pre-Authentication Warning Page*, *Pre-Authentication Warning Message*, and *RADIUS Challeneg Reply-Message*.

The two pre-authentication messages are only available once pre-authentication has been enabled under *System* > *Administration* > *System Access*.

Device Self-enrollment

Device certificate self-enrollment is a method for users to obtain certificates for their devices. It can be used to enable EAP-TLS for BYOD configurations, or for VPN authentication. For more information, see Device self-enrollment on page 1.

Captive portal

The following section describes how you can use FortiAuthenticator to grant remote users access to certain portions of the network using delegated authentication through a captive portal. Authentication requires the user to associate their device with the guest SSID as published by the FortiGate wireless controller.

The FortiGate facilitates access control by redirecting the user's web browser to one of the FortiAuthenticator's captive portals. As such, some FortiGate configuration is required.

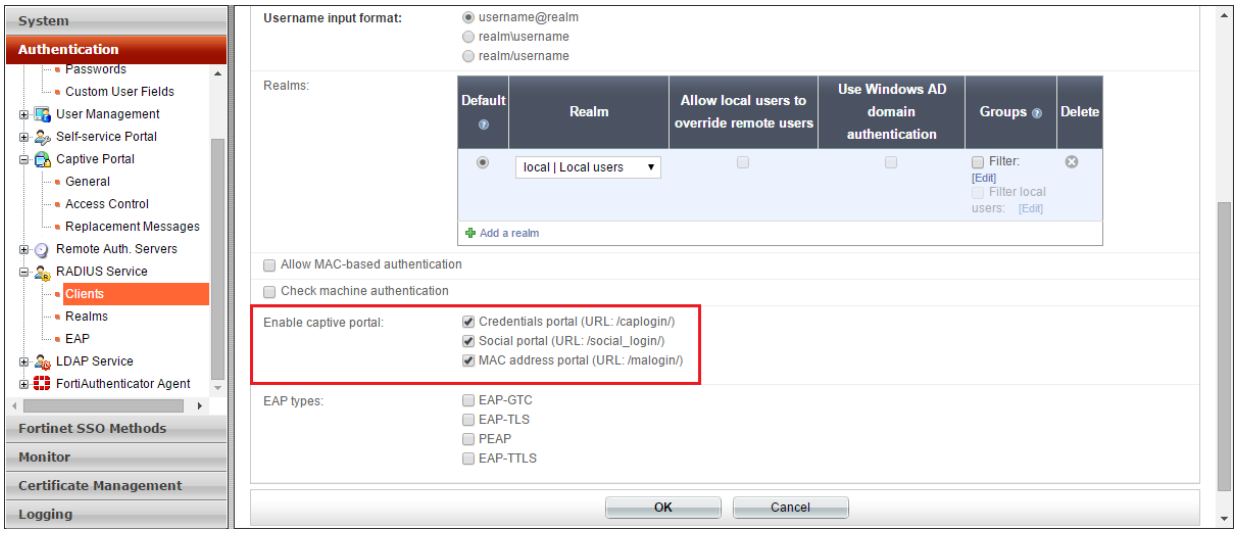
The following captive portal authentication options are available:

- Credentials authentication
- Social WiFi authentication
- MAC address authentication

To enable each captive portal:

Captive portal access is enabled on a per-FortiGate basis through the RADIUS client configuration at *Authentication* > *RADIUS Service* > *Clients* > *Enable captive portal*.

Options are available to enable each captive portal individually:



To configure each captive portal:

General captive portal configuration is available under *Authentication* > *Captive Portal* > *General*.

Credentials authentication

The credentials portal requires known users (users who already have an account) to authenticate using their credentials (password and/or token code). The goal is to restrict access to a set of pre-authorized users only.

For the Credentials portal, the administrator must indicate which of the profiles to use for user authentication. For environments where there is one FortiWifi with multiple access points (AP), the administrator can specify a list of IP addresses for all the APs.

When the user is redirected to the Credentials portal login page, they must enter their username and password, and (optionally) their FortiToken passcode. Upon successful login, the user is redirected to the webpage originally requested.

Social WiFi authentication

Social Wifi authentication allows FortiAuthenticator to utilize third-party user identity methods (social sites, valid e-mail address, or phone number) to authenticate users into a wireless guest network.

The goal is to provide some traceability of users without requiring the heavy overhead of creating guest accounts.

Third-party authentication methods

Supported third-party authentication methods are described in the table below.

Each third-party method can be enabled or disabled on an individual basis under *Authentication* > *Captive Portal* > *General*.

Third-party method	Method description
Google +	Log-in using Google+ is an option for Google users, utilizing the OAUTH2 protocol described here: https://console.developers.google.com/start. Once logged in, the user can *Add to Circles* with the organization.
Facebook	Log-in via Facebook is known as "Facebook Connect" and is described here: https://developers.facebook.com/products/login. Once logged in, the user can *Like* the organization's Facebook page.
LinkedIn	Log-in via Linkedin is supported using the OAUTH2 protocol as described here: https://developer.linkedin.com/documents/authentication. Once logged in, the user can *Connect* with the organization.
Twitter	Log-in via Twitter is supported as described here: https://dev.twitter.com. Once logged in, the user can *Follow* the organization.
Form-based authentication	Similar to the existing Self-registration page, it is possible to register by supplying user details. It is also possible to register using minimal (configurable) information, for example: e-mail or mobile-only. Such information is commonly gathered in short-term transient use locations such as airports and coffee shops.
SMS-based authentication	In SMS-based authentication, the user is redirected to a registration portal which requests a valid mobile phone number. When the user enters their number, a passcode is sent to their mobile device. The user then enters this passcode at the authentication screen to successfully authenticate.
Email-based authentication	Email-based authentication is similar to SMS-based authentication, except that the user enters their email address instead of their mobile phone number. A passcode is then sent to the user's email address. The user enters this passcode into the captive portal registration page.

MAC address authentication

This feature is particularly useful in situations where only the identity of the user is important, for example:

- Wireless guest networks
- Retail environments
- Transient access (airports, hotels, etc.)

The purpose is to identify and authenticate users with minimal interaction from the user, with some traceability of the users. This authentication method is less disruptive and therefore provides a better user experience.

With MAC address authentication enabled, the user attempts to open a web browser but is intercepted by the FortiGate wireless controller, and redirected to the FortiAuthenticator portal configured to record the user's MAC address (without requiring any user interaction). The user is then redirected to the webpage originally requested.

Access Control

The *Access Control* page under *Authentication* > *Captive Portal* provides a consolidated view of which RADIUS client has access to which captive portal(s).

Replacement Messages

Custom login pages for authentication are configurable on a per device, location, or organization basis, allowing the administrator to customize content specific to a brand identity. See *Captive Portal* > *Replacement Messages*.

For example:

- **Default Webpage Portal Login**
  You can change the default webpage portal login at *Authentication* > *Captive Portal* > *Replacement Messages* by simply editing the HTML for the *Captive Portal Login Page* item.
- **Default Social Authentication Login Portal**
  You can change the default social authentication login page at *Authentication* > *Captive Portal* > *Replacement Messages* by simply editing the HTML for the *Captive Portal Social Login Page* item.
- **Terms and Disclaimer Agreement page**
  For all portals, it is possible to require that the user agree to a Terms and Disclaimer Agreement before proceeding to the authentication method. You must enable this requirement for the desired portal under *Captive Portal* > *General*.

  You can change the default disclaimer at *Authentication* > *Captive Portal* > *Replacement Messages* by simply editing the HTML for the *Captive Portal Login Disclaimer Page* item.
- **FortiAuthenticator Splash Page**
  Following a successful login, the FortiGate may be configured to redirect to the FortiAuthenticator splash page. The splash page may contain tools that can improve the customer's social media presence.

  You can change the default splash page at *Authentication* > *Captive Portal* > *Replacement Messages* by simply editing the HTML for the *Captive Portal Splash Screen Page* item.

To edit a replacement message:

1. Select a message in the replacement message list.
2. Edit the plain text or HTML code in the lower right pane, or select the open in new window icon to edit the message in a new browser window.
3. When you are finished editing the message, select *Save* to save your changes.
4. If you have made an error when editing the message, select *Restore Default* to restore the message to its default value.

Manage Images

Images can be managed by selecting *Manage Images* in the *Replacement Messages* window. Images can also be added, deleted, and edited.

To add an image:

1. In the manage images screen, select *Create New* to open the *Create New Image* window.
2. Enter a name for the image in the *Name* field.
3. Select *Browse...*, find the GIF, JPEG, or PNG image file that you are adding, and then select *Open*.
   The maximum image size is 65kB.
4. Select *OK* to add the image.

To delete an image:

1. In the manage images screen, select an image, then select *Delete*.
2. Select *Yes, I'm sure* in the confirmation window to delete the image.

To edit an image:

In the manage images screen, select an image, then select *Edit*.

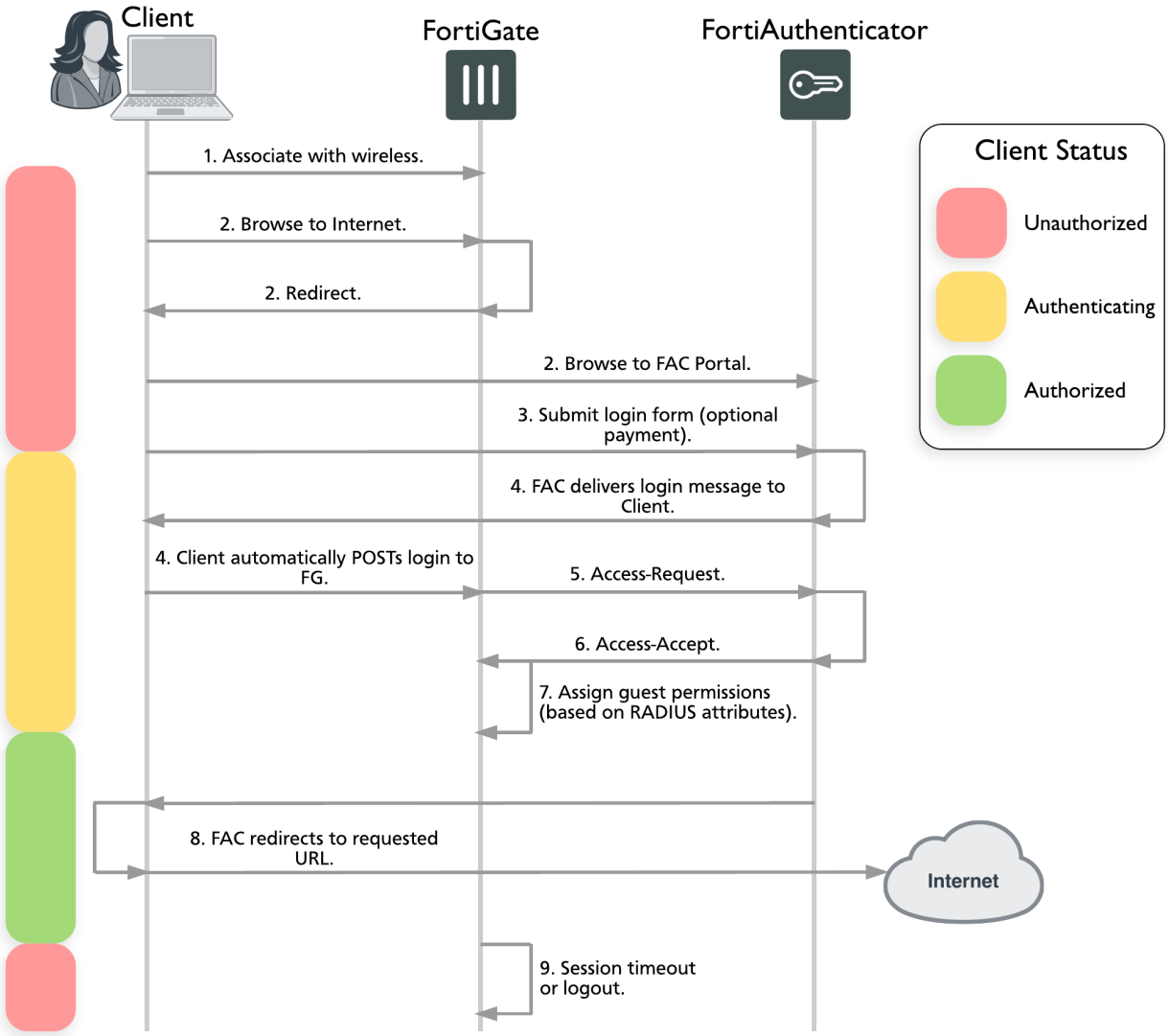
1. In the *Edit Image* window, edit the image name and file as required.
2. Select *OK* to apply your changes.

Account expiry

Account expiry can be configured for Social and MAC Address portals under *Authentication* > *Captive Portal* > *General*. Set the desired timeout next to *Account expires after*.

Account expiry is not available for the Credentials portal.

Captive portal communication workflow example (WiFi)



1. The client associates their Wi-Fi device to the guest SSID as published by the FortiGate wireless controller.
2. The client opens a browser. Based on the configured home page or requested webpage, the initial HTTP traffic is intercepted by the FortiGate wireless controller and redirected to the FortiAuthenticator web login page defined in the FortiGate captive portal profile.
3. The client enters their user credentials on the FortiAuthenticator web login page.FortiAuthenticator performs any pre-authorizationn checks that are required and displays the login message to the guest user. If the client does not have credentials, there may (depending on configuration) be an option to purchase login time.
4. The login message instructs the guest user's browser to submit the user credentials directly to the FortiGate as HTTPS POST for authentication processing.
5. When the FortiGate receives the client credentials in the HTTPS POST, it sends a RADIUS Access-Request to the FortiAuthenticator RADIUS server to authenticate the user.
6. FortiAuthenticator validates the Access-Request message using its user database which can either be local or remote (LDAP/RADIUS).

7. Based on the results of the authentication and authorization processing, FortiAuthenticator responds with either an Access-Accept or Access-Reject message. If the authentication is successful, the Access-Accept message contains one or more RADIUS attributes to define the context of the client session. These attributes can include, but are not limited to: the session duration, bandwidth, and access permissions. When the FortiGate receives the Access-Accept message, it changes the role of the client session allowing the device access to the network.
8. Following a successful authentication and initiation of the user session, the client is redirected to the originally requested URL, which should now be accessible.
9. Based on the Session-Timeout received in the original Access-Accept packet from FortiAuthenticator, the FortiGate counts down the remaining time that is valid for the current guest user session. When the time has expired, or if the user manually terminates the session, FortiGate terminates the session.

FortiGate configuration

In order to allow redirection to an external captive portal and also allow the supply of identifying information about the requesting IP, some FortiGate configuration is required. The example below is configured using the CLI, with the following attributes:

- WAN 1 = Internet
- FAC IP = 192.168.0.122
- Wireless users connecting to "Fortinet" SSID are on the network 10.10.x.x.

Additional non-standard commands to enable the feature are provided in red.

Configuring RADIUS

```
config user radius
   edit "FAC_4.0"
      set server "192.168.0.122"
      set secret ENC
          PGTVcRMZH5mFV2aWl1A1Kbqsr3ZAKcZuEdK5Jsx+2h87uBjyWR1wuU2MY07k4H46ZHuLwBKAky9Zyn0R
          qHEPB3Cku232hFpkOOLlI2gzPnQbPeVcfhC18sxSWvk/fpgDhUTwPoGnYofl9vLrwpPzbkzvJhaXXcgs
          fSTuQ5wxK/5YghiLbdq04nnnTzQd8N8QjsUE5w==
      next
   end
```

Configuration of the accounting server might not be nessesary if the RADIUS Accounting is the same as the RADIUS Auth server.

Configuring the Group

```
config user group
   edit "Wireless_Auth"
      set member "FAC_4.0"
   next
end
```

Configuring VAP

Configure captive portal security with an external Portal rather than the native on-FGT portal.

```
config wireless-controller vap
```

```
    edit "fortinet"
       set vdom "root"
       set security captive-portal
       set selected-usergroups "Wireless_Auth"
       set intra-vap-privacy enable
       set local-switching disable
       set external-web "http://192.168.0.122/caplogin
    next
end
```

Configuring the FAC Address (Group)

Configure the ForiAuthenticator address or group to use as an exemption rule in the firewall policy. This is to allow traffic to flow to the FAC portal to enable authentication when the user is not yet authenticated. This group may also include any servers used to host images referenced on the FAC portal.

```
config firewall address
   edit "FortiAuthenticator"
      set type iprange
      set associated-interface "internal"
      set start-ip 192.168.0.122
      set end-ip 192.168.0.123
   next
end
```

If Social Wifi is enabled, this exemption group will need to consist of all Facebook, Google, LinkedIn, and/or Twitter servers used in the authentication process.

Configuring the Firewall Policy

In these firewall policies, an exemption is made to allow access to the FortiAuthenticator (rule 21) and to external Internet resources (rule 17, "For_SocialWiFi"), which may include content embedded on the portal login page (images, videos, organization website), or may be used in the future to enable exemption for Social Wifi (Google, Facebook, LinkedIn, Twitter).

```
config firewall policy
   edit 21
      set srcintf "fortinet"
      set dstintf "internal"
      set srcaddr "all"
      set dstaddr "FortiAuthenticator"
      set action accept
      set schedule "always"
      set service "ALL"
      set captive-portal-exempt enable
   next
      :
      :
      :
   edit 17
      set uuid 6d71b2b4-4efd-51e4-a21f-272dd0bcdcd9
      set srcintf "fortinet"
      set dstintf "wan1"
      set srcaddr "all"
      set dstaddr "For_SocialWiFi"
```

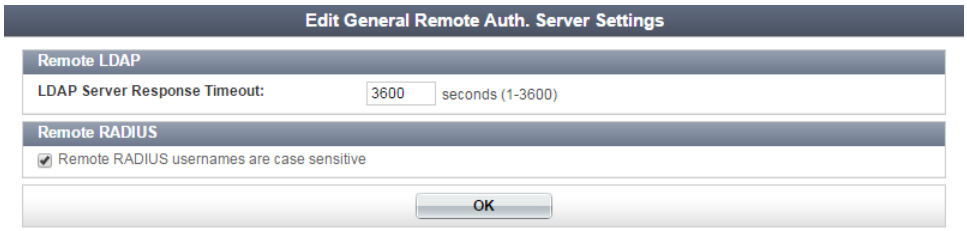
```
        set action accept
        set schedule "always"
        set service "ALL"
        set captive-portal-exempt enable
        set nat enable
    next
end
```

Remote authentication servers

If you already have LDAP or RADIUS servers configured on your network, FortiAuthenticator can connect to them for remote authentication, much like FortiOS remote authentication.

General

Go to *Authentication* > *Remote Auth. Servers* > *General* to configure general remote LDAP and RADIUS server settings (default settings shown in the image below).



The following options are available:

Remote LDAP	Enter a period of time in seconds to configure the LDAP server response timeout. Set the value between 1-3600.
Remote RADIUS	Select to apply case sensitivity for remote RADIUS usernames.

LDAP

If you have existing LDAP servers, you may choose to continue using them with FortiAuthenticator by configuring them as remote LDAP servers.

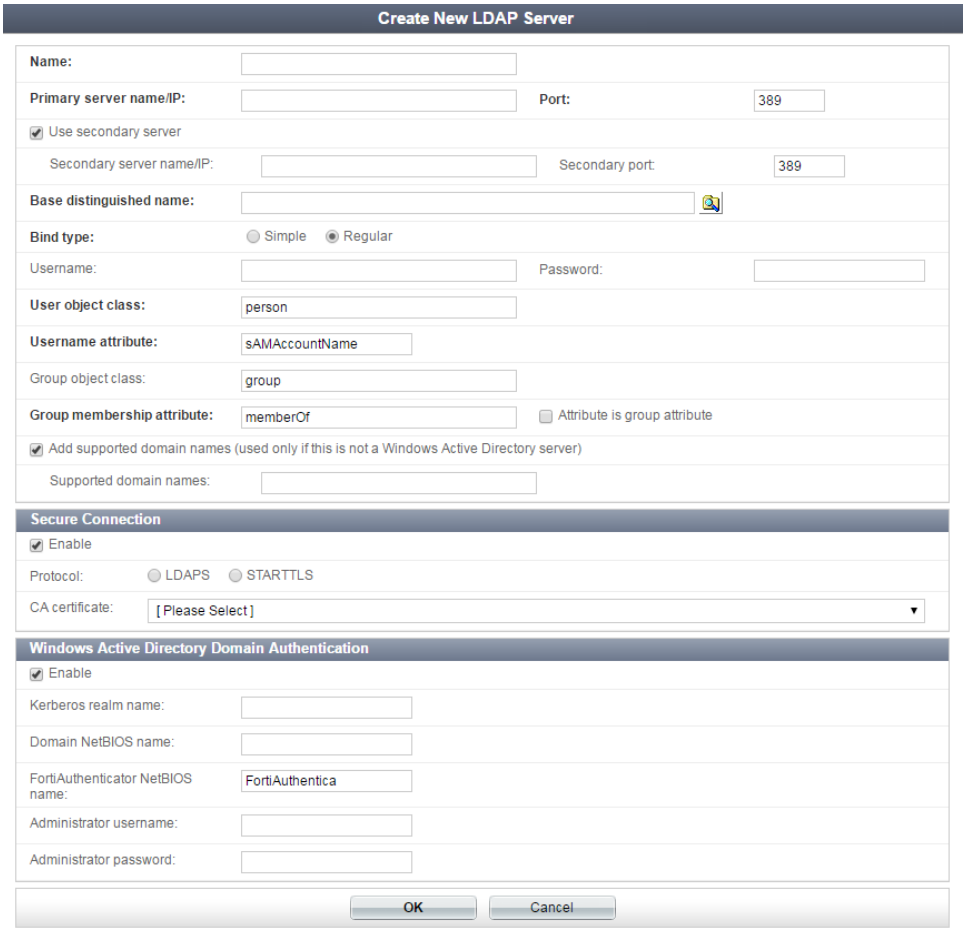
When entering the remote LDAP server information, if any information is missing or in the wrong format, error messages will highlight the problem for you.

As of FortiAuthenticator 4.2, FortiAuthenticator supports multiple Windows AD server forests, with a maximum of 20 Remote LDAP servers with Windows AD enabled.

To view all information about your multiple servers, go to *Monitor* > *Authentication* > *Windows AD*.

To add a remote LDAP server entry:

1. Go to *Authentication* > *Remote Auth. Servers* > *LDAP* and select *Create New*. The *Create New LDAP Server* window opens.



2. Enter the following information.

Name	Enter the name for the remote LDAP server on FortiAuthenticator.
Primary server name/IP	Enter the IP address or FQDN for this remote server.
Port	Enter the port number.
Use secondary server	Select to use a secondary server. The secondary server name/IP and port must be entered.
Secondary server name/IP	Enter the IP address or FQDN for the secondary remote server. This option is only available when *Use secondary server* is selected.
Secondary port	Enter the port number for the secondary server. This option is only available when *Use secondary server* is selected.

Base distinguished name	Enter the base distinguished name for the server using the correct X.500 or LDAP format. The maximum length of the DN is 512 characters. You can also select the browse button to view and select the DN on the LDAP server.
Bind Type	The Bind Type determines how the authentication information is sent to the server. Select the bind type required by the remote LDAP server. • *Simple*: bind using the user's password which is sent to the server in plaintext without a search. • *Regular*: bind using the user's DN and password and then search. If the user records fall under one directory, you can use *Simple* bind type. But *Regular* is required to allow a search for a user across multiple domains.
User object class	The type of object class to search for a user name search. The default is *person*.
Username attribute	The LDAP attribute that contains the user name. The default is *sAMAccountName*.
Group membership attribute	Used as the attribute to search for membership of users or groups in other groups.
Group object class	The type of object class to search for a group name search. The default is *group*.
Add supported domain names (used only if this is not a Windows Active Directory server)	Select to enter multiple domain names for remote LDAP server configurations. The FortiAuthenticator can then identify the domain that users on the LDAP server belong to.

3. If you want to have a secure connection between the FortiAuthenticator unit and the remote LDAP server, under *Secure Connection*, select *Enable*, then enter the following:

Protocol	Select *LDAPS* or *STARTLS* as the LDAP server requires.
CA Certificate	Select the CA certificate that verifies the server certificate from the drop-down list.

4. If you want to authenticate users using MSCHAP2 PEAP in an Active Directory environment, enable *Windows Active Directory Domain Authentication*, then enter the required Windows AD Domain Controller information.

Kerberos realm name	Enter the domain's DNS name in uppercase letters.
Domain NetBIOS name	Enter the domain's DNS prefix in uppercase letters.
FortiAuthentication NetBIOS name	Enter the NetBIOS name that will identify the FortiAuthenticator unit as a domain member.

Administrator username	Enter the name of the user account that will be used to associate the FortiAuthenticator unit with the domain. This user must have at least Domain User privileges.
Administrator password	Enter the administrator account's password.

When you are finished here, go to *Authentication* > *RADIUS Service* > *Clients* to choose whether authentication is available for all Windows AD users or only for Windows AD users who belong to particular user groups that you select. See RADIUS service on page 1 for more information.

5. Select *OK* to apply your changes.
   You can now add remote LDAP users, as described in Remote users on page 1.

Remote LDAP password change

Windows AD users can conveniently change their passwords without provision changes being made to the network by a Windows AD system administrator. There are three ways FortiAuthenticator supports a password change: RADIUS Login, GUI User Login, and GUI User Portal.

RADIUS Login

For the method to work, all of the following conditions must be met:

- FortiAuthenticator has joined the Windows AD domain
- RADIUS client has been configured to "Use Windows AD domain authentication"
- RADIUS authentication request uses MS-CHAPv2
- RADIUS client must also support MS-CHAPv2 password change

A "change password" response will be produced that FortiAuthenticator will recognize, which will allow cooperation between the NAS and the Windows AD server that will result in a password change.

GUI User Login

For this method to work, *one* of the following conditions must be met:

- FortiAuthenticator has joined the Windows AD domain
- Secure LDAP is enabled and the LDAP admin (i.e. regular bind) has the permissions to reset user passwords

You must log in via the GUI portal. FortiAuthenticator will validate the user password against a Windows AD server. The Windows AD server will return with a "change password" response. If that happens, the user will be prompted to enter a new password.

GUI User Portal

For this method to work, *one* of the following conditions must be met:

- FortiAuthenticator has joined the Windows AD domain
- Secure LDAP is enabled

Once successfully logged into the GUI, the user has access to the user portal. If desired, the user can change their password in the user portal.

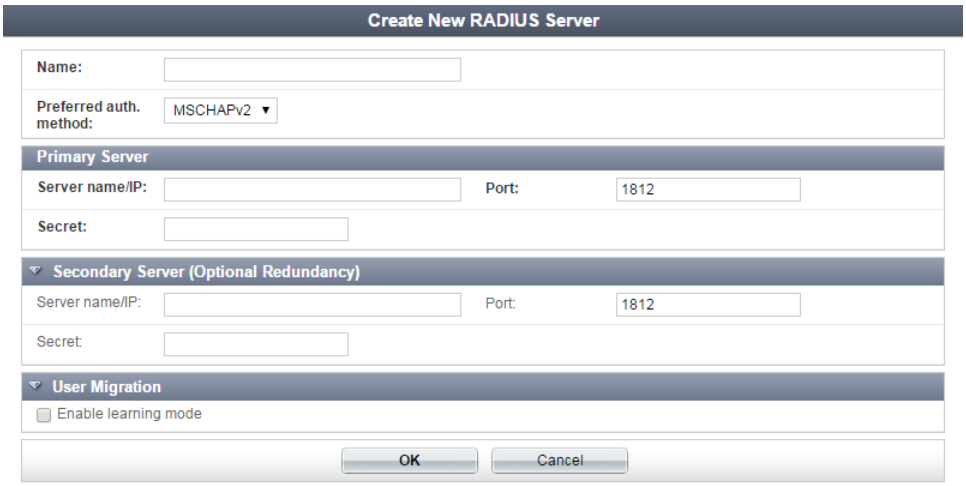
RADIUS

If you have existing RADIUS servers, you may choose to continue using them with FortiAuthenticator by configuring them as remote RADIUS servers.This feature can also be used to migrate away from third party two-factor authentication platforms.

When entering the remote RADIUS server information, if any information is missing or in the wrong format, error messages will highlight the problem for you.

To add a remote RADIUS server entry:

1. Go to *Authentication* > *Remote Auth. Servers* > *RADIUS* and select *Create New*. The *Create New RADIUS Server* window opens.



2. Enter the following information, then select *OK* to add the RADIUS server.

Name	Enter the name for the remote RADIUS server on FortiAuthenticator.
Preferred auth. method	Select the preferred authentication protocol from the dropdown menu: • MSCHAPv2 • MSCHAP • CHAP • PAP
Primary Server	Enter the server name or IP address, port and secret in their requisite locations to configure the primary server.
Secondary Server	Optionally, add redundancy by configuring a secondary server.
User Migration	Select *Enable learning mode* to record and learn users that authenticate against this RADIUS server. This option should be enabled if you need to migrate users from the server to the FortiAuthenticator. Select *View Learned Users* to view the list of learned users. See Learned RADIUS users on page 1.

RADIUS service

Before the FortiAuthenticator unit can accept RADIUS authentication requests from a FortiGate unit, the FortiGate unit must be registered as a authentication client on the FortiAuthenticator unit.

The FortiAuthenticator RADIUS server is already configured and running with default values. Each user account on the FortiAuthenticator unit has an option to authenticate the user using the RADIUS database.

Every time there is a change to the list of RADIUS authentication clients, two log messages are generated: one for the client change, and one to state that the RADIUS server was restarted to apply the change.

FortiAuthenticator unit allows both RADIUS and remote authentication for RADIUS authentication client entries. If you want to use a remote server, you must configure it first so that you can be select it in the RADIUS authentication client configuration, see Remote authentication servers on page 1. You can configure the built-in LDAP server before or after creating client entries, see LDAP service on page 1.

Clients

RADIUS accounting client can be managed from *Authentication* > *RADIUS Service* > *Clients*.

Clients can be added, imported, deleted, edited, and cloned as needed.

To configure a RADIUS accounting client:

1. From the RADIUS client list, select *Create New* to add a new RADIUS client. The *Add RADIUS client* window opens.
2. Enter the following information:

Name	A name to identify the FortiGate unit.
Client name/IP	The FQDN or IP address of the unit.
Secret	The RADIUS passphrase that the FortiGate unit will use.
Description	Optionally, enter information about the FortiGate unit.
Authentication method	Select one of the following: • *Enforce two-factor authentication* • *Apply two-factor authentication if available (authenticate any user)* • *Password-only authentication (exclude users without a password)* • *FortiToken-only authentication (exclude users without a FortiToken)*.
Username input format	**Select one of the following three username input formats:** • *username@realm* • *realm\username* • *realm/username*.

Realms	**Add realms to which the client will be associated. See Realms on page 101.** • Select a realm from the drop-down list in the *Realm* column. • Select whether or not to allow local users to override remote users for the selected realm. • Select whether or not to use Windows AD domain authentication. • Edit the group filter as needed. That is, filter users based on the groups they are in. • If necessary, add more realms to the list. • Select the realm that will be the default realm for this client.
Allow MAC-based authentication	**To allow 802.1X authentication for non-interactive devices, FortiAuthenticator can identify and bypass authentication for a device based on its MAC address. This is used for devices that do not allow the usual username or password input to perform 802.1X authentication, such as network printers. Enter these units in *Authentication* > *User Management* > *MAC Devices*. For more information, see MAC devices on page 1.**
Require Call-Check attribute for MAC-based auth	**The FortiAuthenticator unit expects the username and password attributes to be set to the source MAC address. This option also requires a Service-Type attribute set to *Call Check* and a Calling-Station-Id attribute set to the source MAC address.**
Check machine authentication	**Select to check machine based authentication, and apply groups based on the success or failure of the authentication. See Machine authentication on page 1.**
Override group membership when	**Select the conditions for when a group membership can be overridden from the *Only machine-authenticated* and *Only user-authenticated* drop-down lists.**
EAP types	**Select the 802.1X EAP authentication types to accept. If you require mutual authentication, select EAP-TLS. For more information, see EAP on page 1.**

3. Select *OK* to add the new RADIUS client.

If authentication is failing, check that the authentication client is configured and that its IP address is correctly specified. Common causes of problems are:
- RADIUS packets being sent from an unexpected interface, or IP address.
- NAT being performed between the authentication client and the FortiAuthenticator unit.

Client profile attributes

FortiAuthenticator supports a single authentication profile for each RADIUS Auth Client. Because of this, authentication requirements (for example IPSec/SSLVPN, Web Filtering Override, Wireless Authentication, and

so on) require different profiles, as RADIUS authentication requests originate from the same IP address. To distinguish the authentication requirements, you can add attributes to them.

Attributes (which can be added to authentication requirements) indicate the type of service the user has requested, or the type of service to be provided.

Each FortiAuthenticator Auth Client Profile can contain up to two RADIUS Attributes.

To match a profile, all specified attributes in a profile must match, if not, the processing will fall to the next profile (processed in top down order).

The profiles created can be re-arranged in terms of priority. FortiAuthenticator attempts to match the RADIUS attributes from an authentication request to each profile, starting with the highest-priority profile, and moves down the list until it finds a match. FortiAuthenticator uses the first profile that it matches.

Importing authentication clients

Authentication client information can be imported as a CSV file by selecting *Import* in the from the RADIUS client list.

The CSV file has one record per line, with the record format: client name (32 characters max), FQDN or IP address (128 characters max), secret (optional, 63 characters max).

Realms

Realms allow multiple domains to authenticate to a single FortiAuthenticator unit. They support both LDAP and RADIUS remote servers. Each RADIUS realm is associated with a name, such as a domain or company name, that is used during the log in process to indicate the remote (or local) authentication server on which the user resides.

For example, the username of the user *PJFry*, belonging to the company *P_Express* would become any of the following, depending on the selected format:

- *PJFry@P_Express*
- *P_Express\PJFry*
- *P_Express/PJFry*

The FortiAuthenticator uses the specified realm to identify the back-end RADIUS or LDAP authentication server or servers that are used to authenticate the user.

Acceptable realms can be configured on a per RADIUS server client basis when configured RADIUS service clients. See Clients on page 99.

To manage the realms, go to *Authentication* > *RADIUS Service* > *Realms*.

Create New	Select to create a new realm.
Delete	Select to delete the selected realm or realms.
Edit	Select to edit the selected realm.

Name	The names of the realms.
User Source	The source of the users in the realms.

To create a new realm:

1. From the realms list, select *Create New*. The *Create New Realm* window opens.
2. Enter a name for the realm in the *Name* field.

The realm name may only contain letters, numbers, periods, hyphens, and underscores. It cannot start with a special character.

3. Select the user source for the realm from the User source drop-down list. The options include local users, or users from specific RADIUS or LDAP servers.
4. Select *OK* to create the new realm.

Extensible authentication protocol

The FortiAuthenticator unit supports several IEEE 802.1X EAP methods. EAP settings can be configured from *Authentication* > *RADIUS Service* > *EAP*. See EAP on page 1 for more information.

LDAP service

LDAP is an Internet protocol used to maintain authentication data that may include departments, people, groups of people, passwords, email addresses, and printers. LDAP consists of a data-representation scheme, a set of defined operations, and a request/response network.

In the LDAP protocol there are a number of operations a client can request such as search, compare, and add or delete an entry. Binding is the operation where the LDAP server authenticates the user. If the user is successfully authenticated, binding allows the user access to the LDAP server based on that user's permissions.

General

To configure general LDAP service settings, go to *Authentication* > *LDAP Service* > *General*.

LDAP server certificate	Select the certificate that the LDAP server will present from the drop-down list.
Certificate authority type	Select either *Local CA* or *Trusted CA*.
CA certificate that issued the server certificate	Select the CA certificate that issued the server certificate from the drop-down list.

Select *OK* to apply any changes that you have made.

Directory tree overview

The LDAP tree defines the hierarchical organization of user account entries in the LDAP database. The FortiGate unit requesting authentication must be configured to address its request to the right part of the hierarchy.

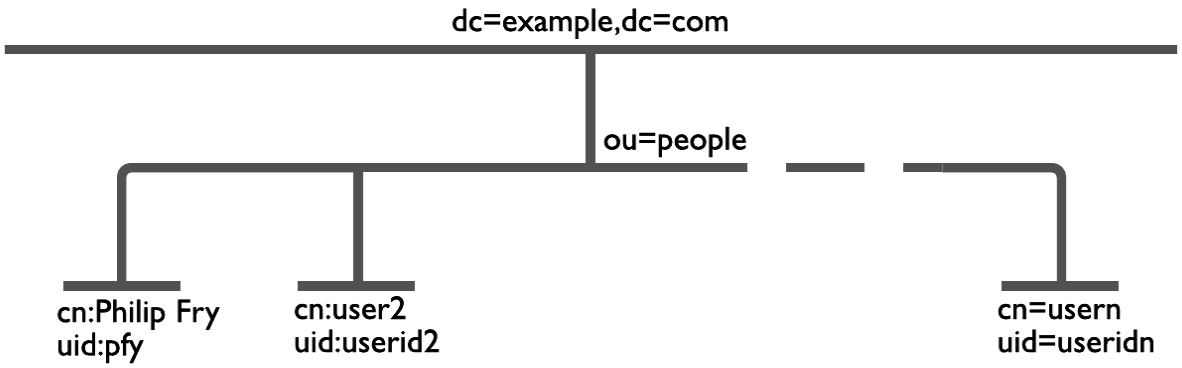
An LDAP server's hierarchy often reflects the hierarchy of the organization it serves. The root represents the organization itself, usually defined as Domain Component (DC), a DNS domain, such as `example.com` (as the name contains a dot, it is written as two parts separated by a comma: `dc=example,dc=com`). Additional levels of hierarchy can be added as needed; these include:

- Country (c)
- User Group (cn)
- Local User (uid)
- Organization (o)
- Organizational Unit (ou)

The user account entries relevant to user authentication will have element names such as user ID (UID) or common name (CN); the user's name. They can each be placed at their appropriate place in the hierarchy.

Complex LDAP hierarchies are more common in large organizations where users in different locations and departments have different access rights. For basic authenticated access to your office network or the Internet, a much simpler LDAP hierarchy is adequate.

The following is a simple example of an LDAP hierarchy in which the all user account entries reside at the Organization Unit (OU) level, just below DC.



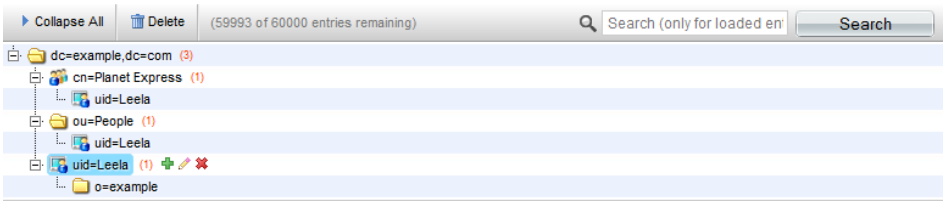
When requesting authentication, an LDAP client, such as a FortiGate unit, must specify the part of the hierarchy where the user account record can be found. This is called the Distinguished Name (DN). In the above example, DN is `ou=People,dc=example,dc=com`.

The authentication request must also specify the particular user account entry. Although this is often called the Common Name (CN), the identifier you use is not necessarily CN. On a computer network, it is appropriate to use UID, the person's user ID, as that is the information that they will provide at logon.

Creating the directory tree

The following sections provide a brief explanation of each part of the LDAP attribute directory, what is commonly used for representation, and how to configure it on FortiAuthenticator.

When an object name includes a space, as in *Test Users*, you have to enclose the text with double-quotes. For example: *cn="Test Users",cn=Builtin,dc=get,dc=local*.



Editing the root node

The root node is the top level of the LDAP directory. There can be only one. All groups, OUs, and users branch off from the root node. Choose a DN that makes sense for your organization's root node.

There are three common forms of DN entries:

The most common consists of one or more DC elements making up the DN. Each part of the domain has its own DC entry. This comes directly from the DNS entry for the organization. For example, for example.com, the DN entry is `"dc=example,dc=com"`.

Another popular method is to use the company's Internet presence as the DN. This method uses the domain name as the DN. For example, for example.com, the DN entry would be `"o=example.com"`.

An older method is to use the company name with a country entry. For example, for Example Inc. operating in the United States, the DN would be `o="Example, Inc.",c=US`. This makes less sense for international companies.

When you configure FortiGate units to use the FortiAuthenticator unit as an LDAP server, you will specify the distinguished name that you created here. This identifies the correct LDAP structure to reference.

To rename the root node:

1. Go to *Authentication* > *LDAP Service* > *Directory Tree*.
2. Select `dc=example,dc=com` to edit the entry.
3. In the *Distinguished Name (DN)* field, enter a new name.
   Example: **`"dc=fortinet,dc=com".`**
4. Select *OK* to apply your changes.

If your domain name has multiple parts to it, such as shiny.widgets.example.com, each part of the domain should be entered as part of the DN, for example: `dc=shiny,dc=widgets,dc=example,dc=com`

Adding nodes to the LDAP directory tree

You can add a subordinate node at any level in the hierarchy as required.

To add a node to the tree:

1. From the LDAP directory tree, select the green plus symbol next to the DN entry where the node will be added. The *Create New LDAP Entry* window opens.
2. In the *Class* field, select the identifier to use.

   For example, to add the `ou=People` node from the earlier example, select *Organizational Unit (ou)*.
3. Select the required value from the drop-down list, or select *Create New* to create a new entry of the selected class.
4. Select *OK* to add the node.

Nodes can be edited after creation by selecting the edit, or pencil, icon next to the node name.

Adding user accounts to the LDAP tree

You must add user account entries at the appropriate place in the LDAP tree. These users must already be defined in the FortiAuthenticator user database. See Adding a user on page 1.

To add a user account to the tree:

1. From the LDAP directory tree, expand nodes as needed to find the required node, then select the node's green plus symbol.

   In the earlier example, you would do this on the `ou=People` node.
2. In the *Class* field, select *User (uid)*.

   The list of available users is displayed. You can choose to display them alphabetically by either user group or user.
3. Select the required users in the *Available Users* box and move them to the *Chosen Users* box. If you want all local users to be added, select *Choose all* below the users box.
4. Select *OK* to add the user account to the tree.

You can verify your users were added by expanding the node to see their UIDs listed below it.

Moving LDAP branches in the directory tree

At times you may want to rearrange the hierarchy of the LDAP structure. For example a department may be moved from one country to another.

While it is easy to move a branch in the LDAP tree, all systems that use this information will need to be updated to the new structure or they will not be able to authenticate users.

To move an LDAP branch:

1. From the LDAP directory tree, select *Expand All* and find the branch that is to be moved.
2. Click and drag the branch from its current location to its new location

   When the branch is hovered above a valid location, an arrow will appear to the left of the current branch to indicate where the new branch will be inserted. It will be inserted below the entry with the arrow.

Removing entries from the directory tree

Adding entries to the directory tree involves placing the attribute at the proper place. However, when removing entries it is possible to remove multiple branches at one time.

Take care not to remove more branches than you intend. Remember that all systems using this information will need to be updated to the new structure or they will not be able to authenticate users.

To remove an entry from the LDAP directory tree:

1. From the LDAP directory tree, select *Expand All* and find the branch that is to be removed.
2. Select the red X to the right of the entry name.
   You will be prompted to confirm your deletion. Part of the prompt displays the message of all the entries that will be removed with this deletion. Ensure this is the level that you intend to delete.
3. Select *Yes, I'm sure* to delete the entry.

If the deletion was successful there will be a green check next to the successful message above the LDAP directory and the entry will be removed from the tree.

Configuring a FortiGate unit for FortiAuthenticator LDAP

When you have defined the FortiAuthenticator LDAP tree, you can configure FortiGate units to access the FortiAuthenticator as an LDAP server and authenticate users.

To configure the FortiGate unit for LDAP authentication:

1. On the FortiGate unit, go to *User & Device* > *Authentication* > *LDAP Server* and select *Create New*.
2. Enter the following information:

Name	Enter a name to identify the FortiAuthenticator LDAP server on the FortiGate unit.
Server Name / IP	Enter the FQDN or IP address of the FortiAuthenticator unit.
Server Port	Leave at default (389).
Common Name Identifier	Enter `uid`, the user ID.
Distinguished Name	Enter the LDAP node where the user account entries can be found. For example, `ou=People,dc=example,dc=com`

Bind Type	The FortiGate unit can be configured to use one of three types of binding: • anonymous - bind using anonymous user search • regular - bind using username/password and then search • simple - bind using a simple password authentication without a search You can use simple authentication if the user records all fall under one distinguished name (DN). If the users are under more than one DN, use the anonymous or regular type, which can search the entire LDAP database for the required username. If your LDAP server requires authentication to perform searches, use the regular type and provide values for *User DN* and *Password*.
Secure Connection	If you select *Secure Connection*, you must select LDAPS or STARTTLS protocol and the CA security certificate that verifies the FortiAuthenticator unit's identity. If you select LDAPS protocol, the Server Port will change to 636.

3. Select *OK* to apply your settings.
4. Add the LDAP server to a user group. Specify that user group in identity-based security policies where you require authentication.

SAML IdP

Security Assertion Markup Language (SAML) is used for exchanging authentication and authorization data between an Identity Provider (IdP) and a Service Provider (SP), such as Google Apps, Office 365, and Salesforce. The FortiAuthenticator can be configured as an IdP, providing trust relationship authentication for unauthenticated users trying to access a SP.

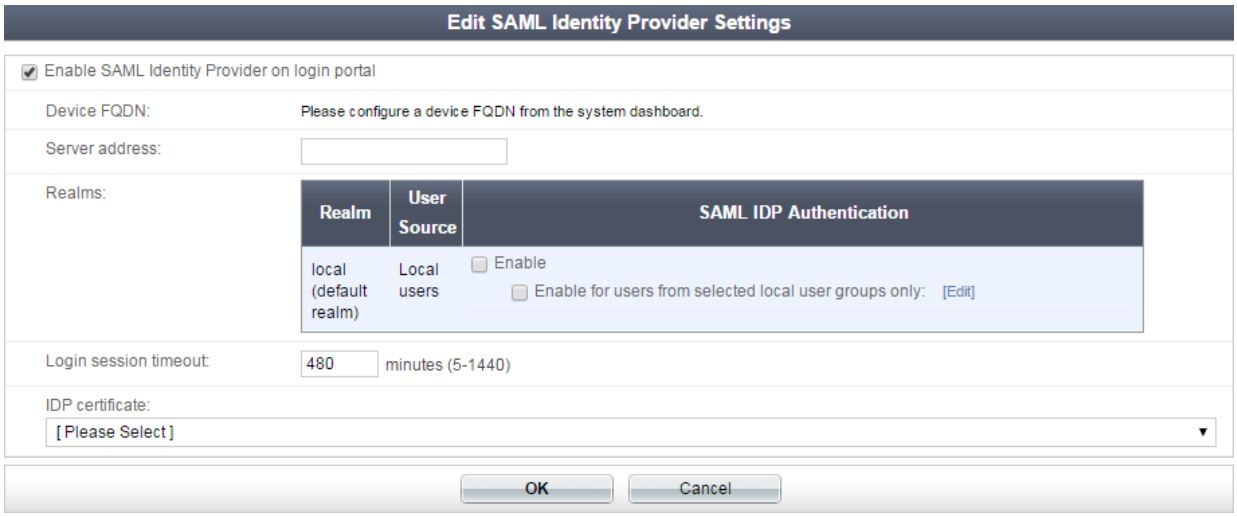
Different realms can be selectively enabled while configuring the FortiAuthenticator as the IdP. These realms are available under *Authentication* > *Self-service Portal* > *Access Control*, where they can be enabled, disabled, or group filtered.

SAML Authentication works as follows:

1. A user tries to access a Service Provider, for example Google, using a browser.
2. The Service Provider's web server requests the SAML assertions for its service from the browser.
3. Two possibilities:
   a. The user's browser already has valid SAML assertions, so it sends them to the Service Provider's web server. The web server uses them to grant or deny access to the service. SAML authentication stops here.
   or
   b. The user's browser doesn't have valid SAML assertions, so the Service Provider's web server redirects the browser to the SAML IdP.
4. Two possibilities:
   a. The user's browser is already authenticated with the IdP, go to step 5.
   b. The user's browser is not yet authenticated with the IdP, IdP requests and validates the user's credentials. If successful, go to step 5. Otherwise, access denied.
5. IdP provides SAML assertions for the Service Provider's and redirects the user's browser back to the Service Provider's web server. Go back to step 2.

General

To configure general SAML IdP portal settings, go to *Authentication* > *SAML IdP* > *General* and select *Enable SAML Identity Provider on login portal*.



Enter the following information:

Device FQDN	To configure this setting, you must enter a *Device FQDN* in the *System Information* widget in the *Dashboard*.
Server address	Enter the IP address, or FQDN, of the FortiAuthenticator device.
Realms	Select *Enable* to add the default local realm to which the users will be associated. Select *Enable for users from selected local user groups only* and select to specify those user groups you want to assign to the realm.
Login session timeout	Set the user's login session timeout limit between 5 - 1440 minutes (480 by default).
IDP certificate	Select a certificate from the dropdown menu.

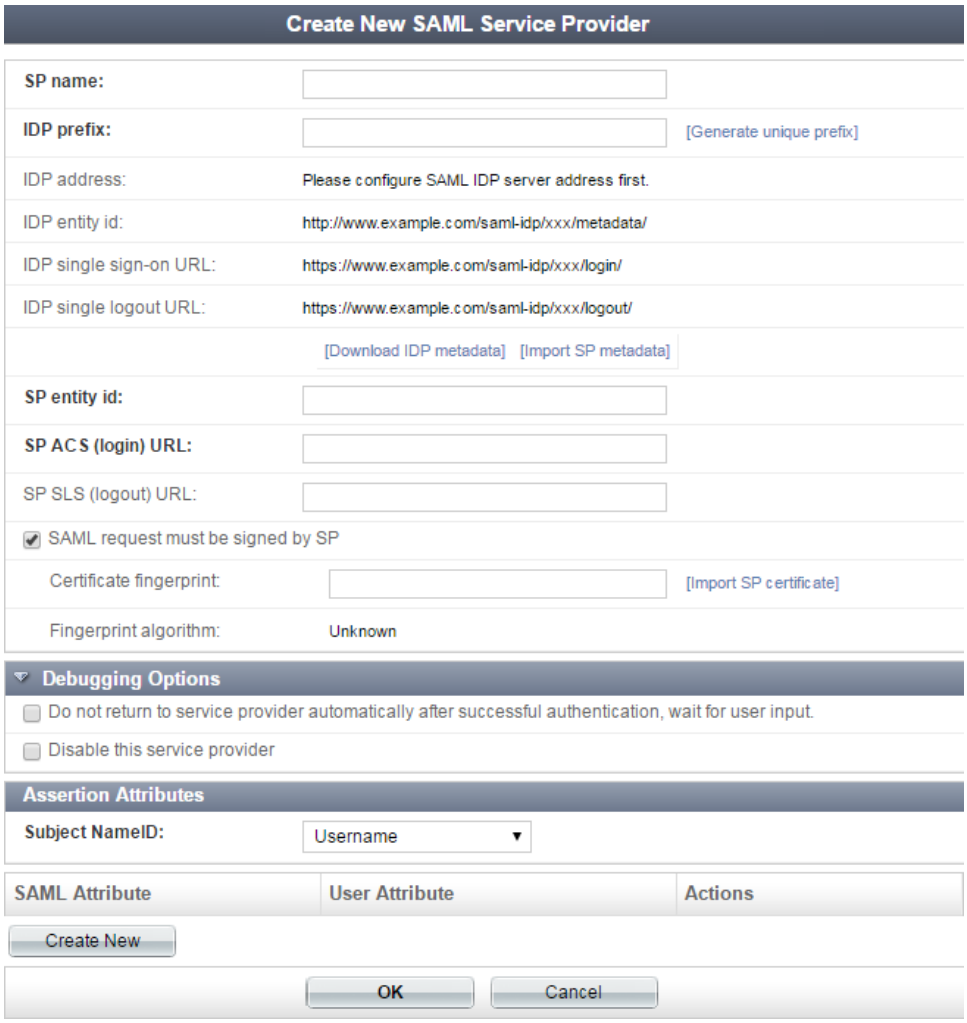
Select *OK* to apply any changes that you have made.

Service Providers

Service Providers can be managed from *Authentication* > *SAML IdP* > *Service Providers*.

To configure a SAML Service Provider:

1. Select *Create New*. The SAML Service Provider window opens.



2. Enter the following information:

SP name	Enter a name for the SP.
IDP prefix	Enter a prefix for the IDP that will be appended to the end of the IDP URLs. Alternatively, you can select *Generate unique prefix* to generate a random 16 digit alphanumerical string.
IDP address	To configure the IDP address (and IDP settings below), you must have already configured the server's address under *Authentication > SAML IdP > General*.
IDP entity id	Configure the IDP's entity id, for example: `http://www.example.com/saml-idp/xxx/metadata/`
IDP single sign-on URL	Configure the IDP's login URL, for example: `http://www.example.com/saml-idp/xxx/login/`

IDP single logout URL	Configure the IDP's logout URL, for example: `http://www.example.com/saml-idp/xxx/logout/`
SP entity id	Enter the SP's entity id
SP ACS (login) URL	Enter the SP's Assertion Consumer Service (ACS) login URL.
SP SLS (logout) URL	Enter the SP's Single Logout Service (SLS) logout URL.
SAML request must be signed	Enable this option and import the SP certificate for authentication request signing by the SP.
Debugging Options	
Do not return to service provider automatically after successful authentication, wait for user input	Enable this option to let users choose where to navigate to once authenticated.
Disable this service provider	Disables the service provider.
Assertion Attributes	
Subject NameID	Select the user attribute that serves as SAML assertion subject NameID. Select from either *Username*, *Email*, or *Remote LDAP user DN*. If the attribute being selected is not available for a user, *Username* will be used by default.

FortiAuthenticator Agents

FortiAuthenticator provides multiple agents for use in two-factor authentication:

- FortiAuthenticator Agent for Microsoft Windows is a credential provider plug-in that allows the Windows login process to be enhanced with a one time password, validated by FortiAuthenticator.
- FortiAuthenticator Agent for Outlook Web Access is a plug-in that allows the Outlook Web login to be enhanced with a one time password, validated by FortiAuthenticator.

Both Agents can be downloaded from the FortiAuthenticator GUI from **Authentication > FortiAuthenticator Agent**.

Port-based Network Access Control

Port-based Network Access Control (PNAC), or 802.1X, authentication requires a client, an authenticator, and an authentication server (such as a FortiAuthenticator device).

The client is a device that wants to connect to the network. The authenticator is simply a network device, such as a wireless access point or switch. The authentication server is usually a host that supports the RADIUS and EAP protocols.

The client is not allowed access to the network until the client's identity has been validated and authorized. Using 802.1X authentication, the client provides credentials to the authenticator, which the authenticator forwards to the authentication server for verification. If the authentication server determines that the credentials are valid, the client device is allowed access to the network.

FortiAuthenticator supports several IEEE 802.1X EAP methods.

EAP

The FortiAuthenticator unit supports several IEEE 802.1X EAP methods. These include authentication methods most commonly used in WiFi networks.

EAP is defined in RFC 3748 and updated in RFC 5247. EAP does not include security for the conversation between the client and the authentication server, so it is usually used within a secure tunnel technology such as TLS, TTLS, or MS-CHAP.

The FortiAuthenticator unit supports the following EAP methods:

Method	Server Auth	Client Auth	Encryption	Native OS Support
PEAP (MSCHAPv2)	Yes	Yes	Yes	Windows XP, Vista, 7
EAP-TTLS	Yes	No	Yes	Windows Vista, 7
EAP-TLS	Yes	Yes	Yes	Windows (XP, 7), Mac OS X, iOS, Linux, Android
EAP-GTC	Yes	Yes	Yes	None (external supplicant required)

In addition to providing a channel for user authentication, EAP methods also provide certificate-based authentication of the server computer. EAP-TLS provides mutual authentication: the client and server authenticate each other using certificates. This is essential for authentication onto an enterprise network in a BYOD environment.

For successful EAP-TLS authentication, the user's certificate must be bound to their account in *Authentication* > *User Management* > *Local Users* (see Local users on page 1) and the relevant RADIUS client in *Authentication* > *RADIUS Service* > *Clients* (see RADIUS service on page 1) must permit that user to authenticate. By default, all local users can authenticate, but it is possible to limit authentication to specified user groups.

The FortiAuthenticator unit and EAP

A FortiAuthenticator unit delivers all of the authentication features required for a successful EAP-TLS deployment, including:

- Certificate Management: create and revoke certificates as a CA. See Certificate Management on page 1.
- Simple Certificate Enrollment Protocol (SCEP) Server: exchange a Certificate Signing Request (CSR) and the resulting signed certificate, simplifying the process of obtaining a device certificate.

FortiAuthenticator unit configuration

To configure the FortiAuthenticator unit, you need to:

1. Create a CA certificate for the FortiAuthenticator unit. See Certificate authorities on page 1.

   Optionally, you can skip this step and use an external CA certificate instead. Go to *Certificate Management* > *Certificate Authorities* > *Trusted CAs* to import CA certificates. See Trusted CAs on page 1.
2. Create a server certificate for the FortiAuthenticator unit, using the CA certificate you created or imported in the preceding step. See End entities on page 1.
3. If you configure EAP-TTLS authentication, go to *Authentication* > *RADIUS Service* > *EAP* and configure the certificates for EAP. See Configuring certificates for EAP on page 112.
4. If SCEP will be used:
   a. Configure an SMTP server to be used for sending SCEP notifications. Then configure the email service for the administrator to use the SMTP server that you created. See E-mail services on page 1.
   b. Go to *Certificate Management* > *SCEP* > *General* and select *Enable SCEP*. Then select the CA certificate that you created or imported in Step 1 in the *Default CA* field and select *OK*. See SCEP on page 1.
5. Go to *Authentication* > *Remote Auth. Servers* > *LDAP* and add the remote LDAP server that contains your user database. See LDAP on page 1.
6. Import users from the remote LDAP server. You can choose which specific users will be permitted to authenticate. See Remote users on page 1.
7. Go to *Authentication* > *RADIUS Service* > *Clients* to add the FortiGate wireless controller as an authentication client. Be sure to select the type of EAP authentication you intend to use. See RADIUS service on page 1.

Configuring certificates for EAP

The FortiAuthenticator unit can authenticate itself to clients with a CA certificate.

1. Go to *Certificate Management* > *Certificate Authorities* > *Trusted CAs* to import the certificate you will use. See Trusted CAs on page 1.
2. Go to *Authentication* > *RADIUS Service* > *EAP*.
3. Select the EAP server certificate from the *EAP Server Certificate* drop-down list.
4. Select the trusted CAs and local CAs to use for EAP authentication from their requisite lists.
5. Select *OK* to apply the settings.

Configuring switches and wireless controllers to use 802.1X authentication

The 802.1X configuration will be largely vendor dependent. The key requirements are:

- RADIUS Server IP: This is the IP address of the FortiAuthenticator
- Key: The preshared secret configured in the FortiAuthenticator authentication client settings
- Authentication Port: By default, FortiAuthenticator listens for authentication requests on port 1812.

Device self-enrollment

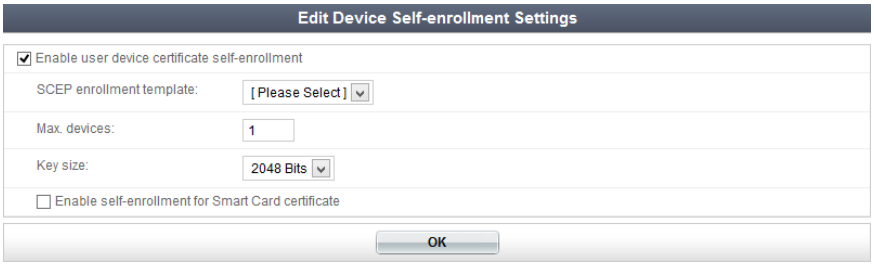
Device certificate self-enrollment is a method for local and remote users to obtain certificates for their devices. It is primarily used in enabling EAP-TLS for BYOD. For example:

- A user brings their tablet to a BYOD organization.
- They log in to the FortiAuthenticator unit and create a certificate for the device.
- With their certificate, username, and password they can authenticate to gain access to the wireless network.
- Without the certificate, they are unable to access the network.

EAP-TLS is a bidirectional certificate authentication method: the client and the FortiAuthenticator EAP need to have matching certificates from the same CA.

To enable device self-enrollment and adjust self-enrollment settings, go to *Authentication* > *Self-service Portal* > *Device Self-enrollment* and select *Enable user device certificate self-enrollment*.

SCEP must be enabled to activate this feature, see SCEP on page 1.



The following settings can be configured:

SCEP enrollment template	Select a SCEP enrollment template from the drop-down list. SCEP can be configured in *Certificate Management* > *SCEP*. See SCEP on page 1 for more information.
Max. devices	Set the maximum number of devices that a user can self-enroll.
Key size	Select the key size for self-enrolled certificates (1024, 2048, or 4096 bits). iOS devices only support two key size: 1024 and 2048.
Enable self-enrollment for Smart Card certificate	Select to enable self-enrollment for smart card certificates. This requires that a DNS domain name be configured, as it is used in the CRL Distribution Points (CDPs) certificate extension.

Select *OK* to apply any changes you have made.

Non-compliant devices

802.1X methods require interactive entry of user credentials to prove a user's identity before allowing them access to the network. This is not possible for non-interactive devices, such as printers. MAC Authentication Bypass is supported to allow non-802.1X compliant devices to be identified and accepted onto the network using their MAC address as authentication.

This feature is only for 802.1X MAC Authentication Bypass. FortiGate Captive Portal MAC Authentication is supported by configuring the MAC address as a standard user, with the MAC address as both the username and password, and not by entering it in the MAC Devices section.

Multiple MAC devices can be imported in bulk from a CSV file. The first column of the CSV file contains the device names (maximum of 50 characters), and the second column contains the corresponding MAC addresses (0123456789AB or 01:23:45:67:89:AB).

To configure MAC-based authentication for a device:

1. Go to *Authentication* > *User Management* > *MAC Devices*. The MAC device list will be shown.
2. If you are adding a new device, select *Create New* to open the *Create New MAC-based Authentication Device* window.

   If you are editing an already existing device, select the device from the device list.
3. Enter the device name in the *Name* field, and enter the device's MAC address in the *MAC address* field.
4. Select *OK* to apply your changes.

To import MAC devices:

1. In the MAC device list, select *Import*.
2. Select *Browse* to locate the CSV file on your computer.
3. Select *OK* to import the list.

   The import will fail if the maximum number of MAC devices has already been reached, or if any of the information contained within the file does not conform, for example if the device name too long, or there is an incorrectly formatted MAC address.

Fortinet Single Sign-On

FSSO is a set of methods to transparently authenticate users to FortiGate and FortiCache devices. This means that the FortiAuthenticator unit is trusting the implicit authentication of a different system, and using that to identify the user. FortiAuthenticator takes this framework and enhances it with several authentication methods:

- Users can authenticate through a web portal and a set of embeddable widgets.
- Users with FortiClient Endpoint Security installed can be automatically authenticated through the FortiClient SSO Mobility Agent.
- Users authenticating against Active Directory can be automatically authenticated.
- RADIUS Accounting packets can be used to trigger an FSSO authentication.
- Users can be identified through the FortiAuthenticator API. This is useful for integration with third party systems.

This section describes FSSO only. For FSSO authentication methods, there is no need to configure anything in the accounting proxy section.

The FortiAuthenticator unit must be configured to collect the relevant user logon data. After this basic configuration is complete, the various methods of collecting the log in information can be set up as needed.

Domain controller polling

When the FortiAuthenticator runs for the first time, it will poll the domain controller (DC) logs backwards until either the end of the log file or the logon timeout setting, whichever is reached first.

When the FortiAuthenticator is rebooted, the memory cache is written to the disk, then re-read at startup, allowing the previous state to be retained. Windows DC polling restarts on boot, then searches backwards in the DC log files until it reaches either the log that matches the last known serial number found in the login cache file, the log that is older than the last recorded read time, or the end of the log file, whichever is reached first.

The currently logged in FSSO users list is cached in memory and periodically written to disk. In an active-passive HA cluster, this file is synchronized to the slave device.

Windows management instrumentation polling

The FortiAuthenticator supports Windows Management Instrumentation (WMI) polling to detect workstation log off. This validates the currently logged on user for an IP address that has been discovered by the DC polling detection method.

Remote WMI access requires that the related ports are opened in the Windows firewall, and access to a domain account that belongs to the Domain Admin group.

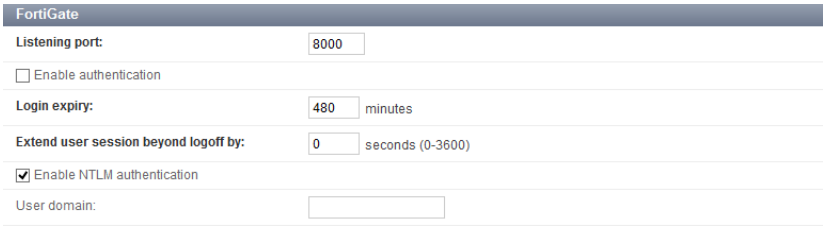
To open ports in the Windows firewall in Windows 7, run `gpedit.msc`, go to *Computer configuration* > *Administrative Templates* > *Network* > *Network Connections* > *Windows Firewall* > *Domain Profile*, go to *Allow remote admin exception*, then enable *remote admin exception* and, if necessary, configure an IP subnet/range.

General settings

The FortiAuthenticator unit listens for requests from authentication clients and can poll Windows Active Directory servers.

To configure FortiAuthenticator FSSO polling:

1. Go to *Fortinet SSO Methods* > *SSO* > *General* to open the *Edit SSO Configuration* window. The *Edit SSO Configuration* window contains sections for FortiGate, FSSO, and user group membership.



2. In the *FortiGate* section, configure the following settings:

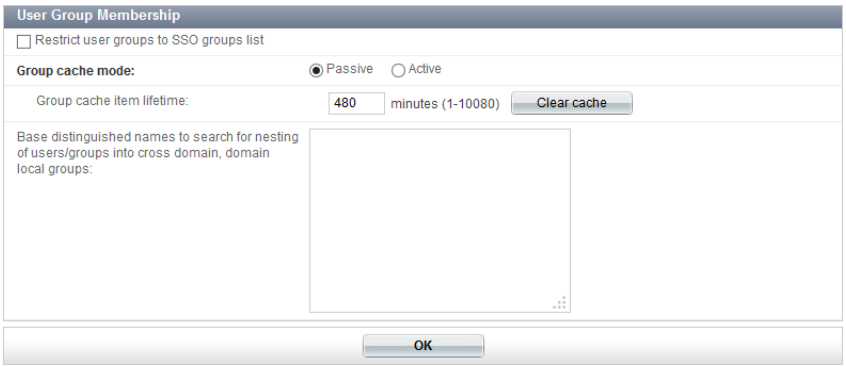
Listening port	Leave at 8000 unless your network requires you to change this. Ensure this port is allowed through the firewall.
Enable authentication	Select to enable authentication, then enter a secret key, or password, in the *Secret key* field.
Login Expiry	The length of time, in minutes, that users can remain logged in before the system logs them off automatically. The default is 480 minutes (8 hours).
Extend user session beyond logoff by	The length of time, in seconds, that a user session is extended after the user logs off, from 0 (default) to 3600 seconds.
Enable NTLM authentication	Select to enable NTLM authentication, then enter the NETBIOS or DNS name of the domain that the login user belongs to in the *User domain* field.

3. In the *Fortinet Single Sign-On (FSSO)* section, configure the following settings:

Maximum concurrent user sessions	Enter the maximum number of concurrent FSSO login sessions a user is allowed to have. Use *0* for unlimited. Select *Configure Per User/Group* to configure the maximum number of concurrent sessions for each user or group. See Fine-grained controls on page 1.
Log Level	Select one of *Debug*, *Info*, *Warning*, or *Error* as the minimum severity level of events to log from the drop-down list. Select *Download all logs* to download all FSSO logs to your management computer.

Enable Windows Active Directory domain controller polling	Select to enable Windows AD polling. Select to enable polling additional logon events, including from devices using Kerberos authentication or from Mac OS X systems, and from event IDs 672, 680, 4776, and 4768.
Enable polling additional logon events	When additional active directory logon event IDs is enabled, event IDs 528, 540, and 4624 are also polled. These event are generated when a user attempts to access a domain service or resource. When a user logs off from the workstation, such an event will be generated. Enter the additional logon event timeout time in the *Additional logon event timeout* field, from 1 to 480 minutes, with 5 minutes being the default time. **Note:** After a user logs off, their SSO session will stay active for the above configured period of time. During this time, if another user changes to the previous user's IP address, they may be able to bypass the necessary authentication. For this reason, it is strongly recommended that the timeout time be kept short.
Enable DNS lookup to get IP from workstation name	Select to use DNS lookup to get IP address information when an event contains only the workstation name. This option is enabled by default.
Directly use domain DNS suffix in lookup	Select to use the domain DNS suffix when doing a DNS lookup. This option is disabled by default.
Enable reverse DNS lookup to get workstation name from IP	Select to enable reverse DNS lookup. Reverse DNS lookup is used when an event contains only an IP address and no workstation name. This option is enabled by default.
Do one more DNS lookup to get full list of IPs after reverse lookup of workstation name	Reverse DNS lookup is used when an event contains only an IP address and no workstation name. Once the workstation name is determined, it is used in the DNS lookup again to get more complete IP address information. This is useful in environments where workstations have multiple network interfaces. This option is disabled by default.
Include account name ending with $ (usually computer account)	Accounts that end in "$" used to exclusively denote computer accounts with no actual user, but in some cases, valid accounts imported from dated systems can feature them. This option is disabled by default.
Enable Radius Accounting SSO clients	Select to enable the detection of users sign-ons and sign-offs from incoming RADIUS accounting (Start, Stop, and Interim-Update) records.
Use RADIUS realm as Windows Active Directory domain	Select to use the RADIUS realm as the Windows AD domain.
Enable Syslog SSO	Select to enable Syslog SSO.

Enable FortiClient SSO Mobility Agent Service	Select to enable single sign-on (SSO) by clients running FortiClient Endpoint Security. For more information, see FortiClient SSO Mobility Agent on page 1.
FortiClient listening port	Enter the FortiClient listening port number.
Enable authentication	Select to enable authentication, then enter a secret key, or password, in the *Secret key* field.
Keep-alive interval	Enter the duration between keep-alive transmissions, from 1 to 60 minutes. Default is 5 minutes.
Idle timeout	Enter an amount of time after which to logoff a user if their status is not updated. The value cannot be lower than the *Keep-alive interval* value.
Enable NTLM	Select to enable the NT LAN Manager (NTLM) to allow logon of users who are connected to a domain that does not have the FSSO DC Agent installed. Disable NTLM authentication only if your network does not support NTLM authentication for security or other reasons. Enter an amount of time after which NTLM authentication expires in the *NTLM authentication expiry* field, from 1 to 10080 minutes (7 days).
Enable hierarchical FSSO tiering	Select to enable hierarchical FSSO tiering. Enter the collector listening port in the *Collector listening port* field.
Enable DC/TS Agent Clients	Select to enable clients using DC or TS Agent. Enter the UDP port in the *DC/TS Agent listening port* field. Default is 8002. Select *Enable authentication* to enable authentication, then enter a secret key, or password, in the *Secret key* field.
Restrict auto-discovered domain controllers to configured domain controllers	Select to enable restricting automatically discovered domain controllers to already configured domain controllers only. See Domain controllers on page 1.
Enable Windows Active Directory workstation IP verification	Select to enable workstation IP verification with Windows Active Directory. If enabled, select *Enable IP change detection via DNS lookup* to detect IP changes via DNS lookup.



4. In the *User Group Membership* section, configure the following settings:

Group cache mode	Select the group cache mode: • *Passive*: Items have an expiry time after which the are removed and re-queried on the next logon. • *Active*: Items are periodically updated for all currently logged on users.
Group cache item lifetime	Enter the amount of time after which items will expire (default = 480 minutes). This is only available when the group cache mode is set to *Passive*.
Do not use cached groups...	Select to prevent using cached groups and to always load groups from server for the following SSO sources: • Windows Active Directory domain controller polling • RADIUS Accounting SSO • Syslog SSO • FortiClient SSO Mobility Agent • DC Agent • TS Agent • User login portal • SSO web service
Base distinguished names to search...	Enter the base distinguished names to search for nesting of users or groups into cross domain and domain local groups.

5. Select *OK* to apply the settings.

Configuring FortiGate units for FSSO

Each FortiGate unit that will use FortiAuthenticator to provide Single Sign-On authentication must be configured to use the FortiAuthenticator unit as an SSO server.

To configure Single Sign-On authentication on the FortiGate unit:

1. On the FortiGate unit, go to *User & Device* > *Authentication* > *Single Sign-On* and select *Create New*.
2. In the *Type* field, select *Fortinet Single-Sign-On Agent*.
3. Enter a name for the FortiAuthenticator unit in the *Name* field.
4. In the *Primary Agent IP/Name* field, enter the IP address of the FortiAuthenticator unit.
5. In the *Password* field, enter the secret key that you defined for the FortiAuthenticator unit. See Enable authentication on page 116.
6. Select *OK*.

   In a few minutes, the FortiGate unit receives a list of user groups from the FortiAuthenticator unit. When you open the server, you can see the list of groups. The groups can be used in identity-based security policies.

Portal services

The SSO portal supports a logon widget that you can embed in any web page. Typically, an organization would embed the widget on its home page.

The SSO portal sets a cookie on the user's browser. When the user browses to a page containing the login widget, the FortiAuthenticator unit recognizes the user and updates its database if the user's IP address has changed. The user will not need to re-authenticate until the login timeout expires, which can be up to 30 days. To log out of FSSO immediately, the user can select the Logout button in the widget.

The SSO portal supports multiple authentication methods including manual authentication, embeddable widgets, and Kerberos authentication.

To configure portal services, go to *Fortinet SSO Methods* > *SSO* > *Portal Services*.

The following settings can be configured:

User Portal		Select *Enable SSO login portal* to enable the SSO login portal.
	Username input format	Select one of the following three username input formats: • *username@realm* • *realm\username* • *realm/username*.
	Realms	Add realms to which the client will be associated. See Realms on page 1. • Select a realm from the drop-down list in the *Realm* column. • Select whether or not to allow local users to override remote users for the selected realm. • Select whether or not to use Windows AD domain authentication. • Edit the group filter as needed. That is, filter users based on the groups they are in. • If necessary, add more realms to the list. • Select the realm that will be the default realm for this client.
	Login timeout	Set the maximum number of days a user is allowed to stay logged in before being logged out automatically from SSO, from 1 to 30 days. Default of 7 days.
	Delay when redirecting to an external URL	Set the delay that occurs when redirecting to an external URL, from 1 to 10 seconds, with a default of 7 seconds.
	Embeddable login widget	Use this code to embed the login widget onto your site. The code cannot be edited manually in this field.
	Login widget demo	A demo of what the login widget will look like on your site.

Kerberos User Portal	Select *Enable Kerberos login for SSO* to enable kerberos log in for SSO. See Kerberos on page 121 for more information.
Import Keytab	Select to open the *Import Keytab* window where you can import a keytab from your computer. A keytab must be imported for Kerberos log in for SSO to be enabled.
Kerberos Principal	Enter the Kerberos principal.
SSO Web Service	Select *Enable SSO Web Service* to use the web service to log users in and out.
SSO user type	Specify the type of user that the client will provide: external, local, or remote (LDAP server must be selected from the drop-down list).

Kerberos

Kerberos authentication allows the FortiAuthenticator to identify connecting users through a Kerberos exchange after a redirect from a FortiGate device.

A keytab file that describes your Kerberos infrastructure is required. To generate this file, you can use a ktpass utility. The following code can be used in a batch file to simplify the keytab file creation:

```
set OUTFILE=fac.keytab
set USERNAME=fac@corp.example.com

set PRINC=HTTP/fac.corp.example.com@CORP.EXAMPLE.COM
set CRYPTO=all

set PASSWD=Pa$$p0rt
set PTYPE=KRB5_NT_PRINCIPAL

ktpass -out %OUTFILE% -pass %PASSWD% -mapuser %USERNAME% -princ %PRINC% -crypto %CRYPTO% -
    ptype %PTYPE%
```

The FortiGate device can be configured to redirect unauthenticated users to the FortiAuthenticator, however the Kerberos authentication URL is different than the standard login URL. The Custom Message HTML for the Login Page HTML Redirect for Kerberos is as follows:

```
<!DOCTYPE HTML>
<html lang="en-US">
   <head>
      <meta charset="UTF-8">
      <meta http-equiv="refresh" content="1;url=http://<fac-fqdn>/login/kerb-auth?user_
          continue_url=%%PROTURI%%">
      <script type="text/javascript">
         window.location.href = http://<fac-fqdn>/login/kerb-auth?user_continue_
             url=%%PROTURI%%
      </script>
      <title>
         Page Redirection
      </title>
   </head>
```

```
    <body>
       If you are not redirected automatically, click on the link
       <a href='http://<fac-fqdn>/login/kerb-auth?user_continue_url=%%PROTURI%%'>
       http://<fac-fqdn>/login/kerb-auth?user_continue_url= %%PROTURI%%
       </a>
    </body>
</html>
```

SAML Service Provider SSO

Security Assertion Markup Language (SAML) is an XML standard that allows for maintaining a single repository for authentication amongst internal and/or external systems.

The FortiAuthenticator can act as a Service Provider (SP) to request user identity information from a third-party Identity Provider (IDP). This information can then be used to sign the user on transparently based on what information the IDP sends.

In this scenario:

1. A user attempts to connect to the Internet via FortiGate
2. The user is not authenticated in FSSO so gets redirected to FortiAuthenticator
3. FortiAuthenticator (a service provider) checks with the existing third party IDP to get the user identity
4. FortiAuthenticator pushes identity and group information into FSSO
5. FortiAuthenticator redirects the user to the original URL
6. FortiGate sees the user in FSSO and allows the user to pass

To configure SAML Portal settings, go to *Fortinet SSO Methods* > *SSO* > *SAML Authentication*, and select *Enable SAML portal*.

The following settings can be configured:

Device FQDN	Enter the FQDN of the configured device from the system dashboard.
Portal url	Enter the Portal URL, for example: *http://www.example.com/login/saml-auth*
Entity id	Enter the Entity ID, for example: *http://www.example.com/metadata/*
ACS (logout) url	Enter the Assertion Consumer Service (ACS) logout URL, for example: *https://www.example.com/saml/?acs*
Download SP metadata	Select to load the service provider SAMLv2 metadata, which will be used for exchanging data with remote parties. All SAMLv2 protocol URLs will be recognized.
Import IDP metadata	Select to import a datafile of the identity provider.

Import IDP certificate	Select to import the certificate of the identity provider.
IDP entity id	Also known as the entity descriptor. Enter the unique name of the SAML identity provider, typically an absolute URL: *https://idp_name.example.edu/idp*
IDP single sign-on URL	Enter the identity provider portal URL you wish to use for single sign-on.

IDP certificate fingerprint	Enter the fingerprint of the certificate file. To calculate the fingerprint, you can use OpenSSL.
	Use the following OpenSSL command:
	`$ openssl x509 -noout -fingerprint -in "server.crt"`
	Example result:
	`SHA1 Fingerprint=AF:E7:1C:28:EF:74:0B:C8:74:25:BE:13:A2:26:3D:37:97:1D:A1:F9`
	In the example above, the fingerprint would be:
	`AF:E7:1C:28:EF:74:0B:C8:74:25:BE:13:A2:26:3D:37:97:1D:A1:F9`

Enable SAML single logout	Select to enable *SLS (logout) url* and set *IDP single logout URL*.
Sign SAML requests with a local certificate	Select to choose a local SAML certificate.
List of IDP groups	Enter SAML identity provider groups. Use their fully distinguished names.
Add all SAML users to SSO group	Select to enter the default SSO group to which SAML users will be added to.

Fine-grained controls

The *Fine-grained Controls* menu provides options to include or exclude a user or group from SSO, and set the maximum number of concurrent sessions that a user or group can have.

To adjust the controls, go to Fortinet *SSO Methods* > *SSO* > *Fine-grained Controls*.

The following options are available:

Edit	Edit the selected user's or group's settings.
Clear Configuration	Clear the SSO configuration for the selected users or groups.
Exclude from SSO	Select a user or users, then select *Exclude from SSO* to exclude them from SSO.
Include in SSO	Select a user or users, then select *Include in SSO* to include the selected users in SSO.
SSO Type	Select the SSO type to view from the drop-down list. The options are: *Local Users*, *Local Groups*, *SSO Users*, and *SSO Groups*.
SSO Name	The users' or groups' names. Select the column title to sort the list by this column.
Maximum Concurrent Sessions	The maximum concurrent sessions allowed for the user or group. This number cannot be greater than five.
Excluded from SSO	If the user or group is excluded from SSO, a red circle with a line will be displayed.

To edit an SSO user or group:

1. In the *Fine-grained Controls* window, select the SSO user or group that is being edited then select *Edit*. The *Edit SSO Item* window opens.
2. Enter the maximum number of concurrent SSO logon sessions per user that the user or group is allowed to have. Enter *0* for unlimited. The number must be equal to or less than five.
3. If the SSO item is a user, select *Exclude from SSO* to exclude the user from SSO.
4. Select *OK* to apply the changes.

SSO users and groups

To manage SSO users and groups, go to *Fortinet SSO Methods* > *SSO* > *SSO Users* or *Fortinet SSO Methods* > *SSO* > *SSO Groups*.

The following options are available:

Create New	Select to create a new user or group. In the *Create New SSO User* or *Create New SSO Group* window, enter a name for the user or group, then select *OK*.
Import	Import SSO users or groups from a remote LDAP server.
Delete	Delete the selected users or groups.

Edit	Edit the selected user or group.
Name	The SSO user or group names.

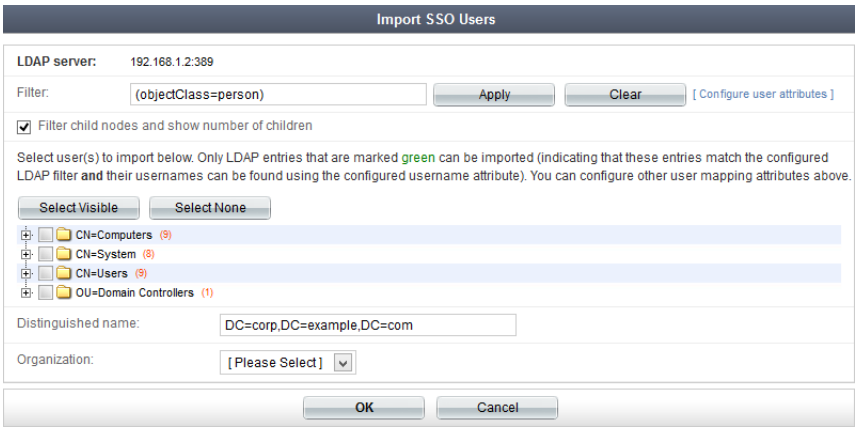
FortiAuthenticator SSO user groups cannot be used directly in a security policy on a FortiGate device. An FSSO user group must be created on the FortiGate unit, then the FortiAuthenticator SSO groups must be added to it. FortiGate FSSO user groups are available for selection in identity-based security policies. See the *FortiOS Handbook* for more information.

To import SSO users or groups:

1. In the *SSO Users* or *SSO Groups* list, select *Import*.
2. In the *Import SSO Users* or *Import SSO Groups* window, select a remote LDAP server from the *Remote LDAP Server* drop-down list, then select *Browse*.

An LDAP server must already be configured to select it in the drop-down list. See LDAP service on page 1 for more information on adding a remote LDAP server.

The *Import SSO Users* or *Import SSO Groups* window opens in a new browser window.



3. Optionally, enter a *Filter* string to reduce the number of entries returned, and then select *Apply*, or select *Clear* to clear the filters.

   For example, `uid=j*` returns only user IDs beginning with "`j`".

4. The default configuration imports the attributes commonly associated with Microsoft Active Directory LDAP implementations. Select *Configure user attributes* to edit the remote LDAP user mapping attributes.

   Selecting the field, *FirstName* for example, presents a list of attributes which have been detected and can be selected. This list is not exhaustive and additional, non-displayed attributes may be available for import. Consult your LDAP administrator for a list of available attributes.

5. Select the entries you want to import.
6. Optionally, select an organization from the *Organization* drop-down to associated the imported users with a specific organization. See Organizations on page 1.
7. Select *OK* to import the users or groups.

Windows Event Log Sources

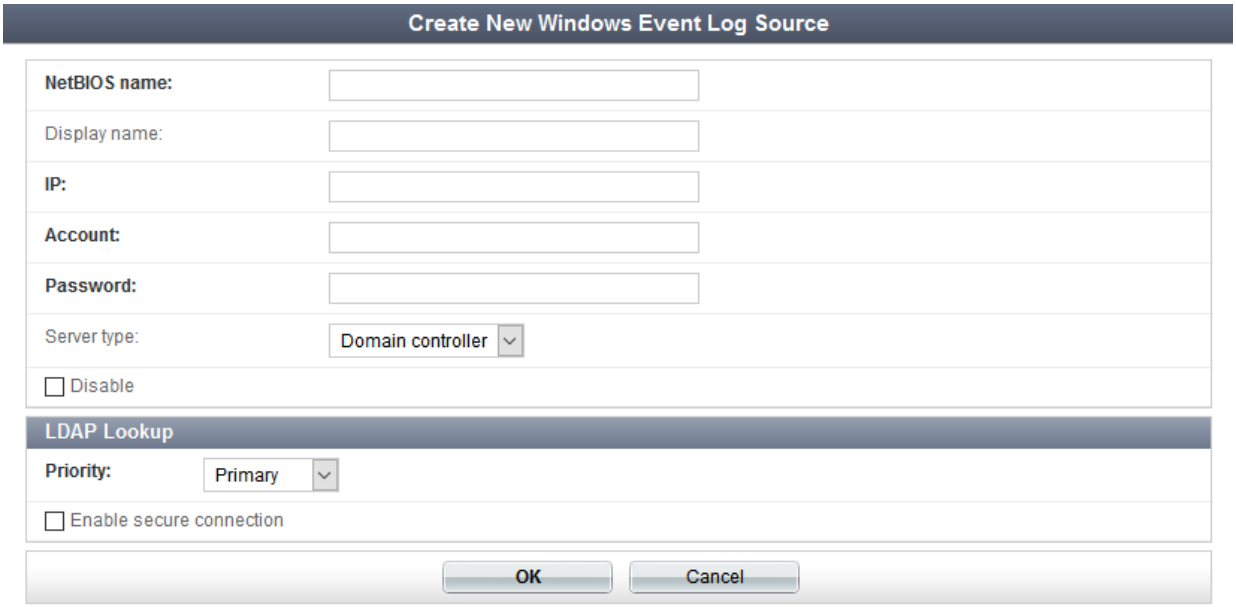
If Active Directory will be used to ascertain group information, the FortiAuthenticator unit must be configured to communicate with the domain controller.

A domain controller entry can be disabled without deleting its configuration. This can be useful when performing testing and troubleshooting, or when moving controllers within your network.

In order to properly discover the available domains and domain controllers, the DNS settings must specify a DNS server that can provide the IP addresses of the domain controllers. See DNS on page 1.

To add a domain controller:

1. Go to *Fortinet SSO Methods* > *SSO* > *Windows Event Log Sources*.
2. Select *Create New* to open the *Create New Windows Event Log Source* window.



3. Enter the following information:

NetBIOS Name	Enter the name of the Domain Controller as it appears in NetBIOS.
Display name	This is a unique name to easily identify this Domain Controller.
IP:	Enter the network IP address of the controller.
Account	Enter the account name used to access logon events. This account should have administrator rights.
Password	Enter the password for the above account.

Server type	Select Domain Controller or Exchange Server as the server type.
Disable	Disable the domain controller without losing any of its settings.
Priority	You can define two (or more) Domain Controllers for the same domain. Each can be designated *Primary* or *Secondary*. The *Primary* unit is accessed first.
Enable secure connection	Select to enable a secure connection.

4. Select OK.

By default, FortiAuthenticator uses auto-discovery of Domain Controllers. If you want to restrict operation to the configured domain controllers only, go to *Fortinet SSO Methods* > *SSO* > *General* and select *Restrict auto-discovered domain controllers to configured domain controllers*. See General settings on page 1.

RADIUS accounting

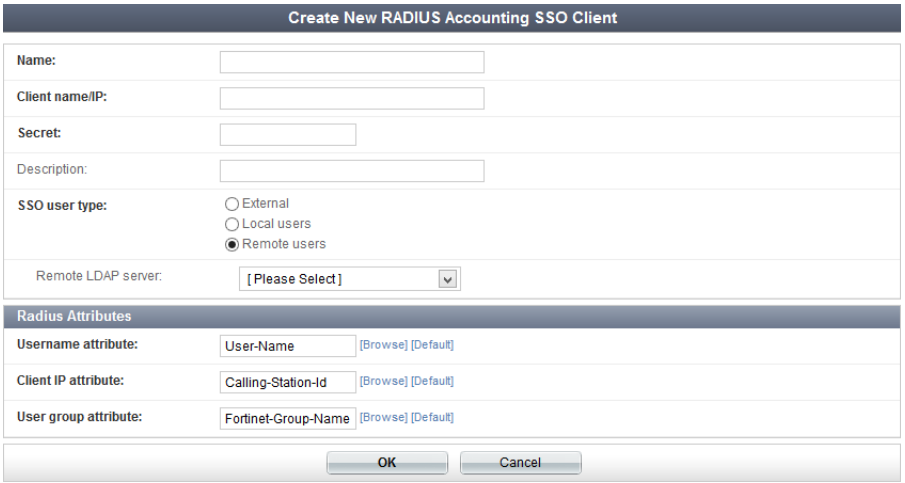
If required, SSO can be based on RADIUS accounting records. The FortiAuthenticator receives RADIUS accounting packets from a carrier RADIUS server or network device, such as a wireless controller, collects additional group information, and then inserts it into FSSO to be used by multiple FortiGate or FortiCache devices for identity based policies.

The FortiAuthenticator must be configured as a RADIUS accounting client to the RADIUS server.

To view the RADIUS accounting SSO client list, go to *Fortinet SSO Methods* > *SSO* > *RADIUS Accounting*.

To configure and enable a RADIUS accounting client:

1. From the RADIUS accounting SSO client list, select *Create New*. The *Create New RADIUS Accounting SSO Client* window opens.



2. Enter the following information:

Name	Enter a name in the *Name* field to identify the RADIUS accounting client on the FortiAuthenticator.
Client name/IP	Enter the RADIUS accounting client's FQDN or IP address.
Secret	Enter the RADIUS accounting client's preshared key.
Description	Optionally, enter a description of the client.
SSO user type	Specify the type of user that the client will provide: external, local, or remote (LDAP server must be selected from the drop-down list).
Radius Attributes	If required, customize the username, client IP, and user group RADIUS attributes to match the ones used in the incoming RADIUS accounting records. See RADIUS attributes on page 1.

3. Select *OK* to apply the changes.
4. Enable RADIUS accounting SSO clients by going to *Fortinet SSO Methods* > *SSO* > *General* and selecting *Enable RADIUS Accounting SSO clients*. See General settings on page 1.

Syslog

The FortiAuthenticator can parse username and IP address information from a syslog feed from a third party device, and inject this information into FSSO so it can be used in FortiGate and FortiCache identity based policies.

Syslog objects include sources and matching rules. Sources identify the entities sending the syslog messages, and matching rules extract the events from the syslog messages. Messages coming from non-configured sources will be dropped.

To configure syslog objects, go to *Fortinet SSO Methods* > *SSO* > *Syslog*.

Syslog SSO must be enabled for this menu option to be available. Go to *Fortinet SSO Methods* > *SSO* > *General* to enable Syslog SSO. See General settings on page 1.

The following options and information are available:

Create New	Create a new syslog source or matching rule.
Delete	Select to delete the selected object or objects.
Edit	Select to edit the selected object.
Syslog SSO Items	Select *Syslog Sources* or *Matching Rules* from the drop-down list.
Name	The name of the source or rule.
Client name/IP	The IP address or the client.

Matching rules

A matching rule is a query, or policy, that is applied to a syslog message in order to determine required information, such as the username and IP address. Rules are required for every syslog source.

Predefined rules are available for Cisco and Aruba wireless controllers (see Predefined rules on page 131). For other systems, custom policies can be created to parse message files in various formats.

To create a new matching rule:

1. In the syslog list, select *Matching Rules* from the *Syslog SSO Items* drop-down menu.
2. Select *Create New*. The *Create New Matching Rule* page ones.
3. Enter the following information:

Name	Enter a name for the source.
Description	Optionally, enter a description of the rule.
Fields to Extract	Configure the fields that are to be extracted from the message.
Trigger	Optionally, enter a string that must be present in all syslog messages. This will act as a pre-filter.
Auth Type Indicators	Enter strings to differentiate between the types of user activities: *Login*, *Update* (optional), and *Logout* (optional).
Username field	Define the semantics of the username field. For example: `User-Name={{user}},` Where {{user}} indicates where the username is extracted from.
Client IP field	Define the semantics of the client IP address.
Group field	Optionally, define the semantics of the group. The group may not always be included in the syslog message, and may need to be retrieved from a remote LDAP server.
Test Rule	Paste a sample log message into the text box, then select *Test* to test that the desired fields are correctly extracted.

4. Select *OK* to add the new matching rule.

Syslog sources

Each syslog source must be defined for traffic to be accepted by the syslog daemon. Each source must also be configured with a matching rule that can be either pre-defined or custom built.

To add a new syslog source:

1. In the syslog list, select *Syslog Sources* from the *Syslog SSO Items* drop-down menu.
2. Select *Create New*. The *Create New Syslog Source* page ones.
3. Enter the following information:

Name	Enter a name for the source.
IP Address	Enter the IP address of the source.
Matching Rule	Select the requisite matching rule from the drop-down list. A matching must already be created for the source.
SSO User Type	Select the SSO user type: • *External*: Users are not defined on the FortiAuthenticator and user groups come from the source. • *Local users*: Users are defined on the FortiAuthenticator as local users, and user groups are retrieved from the local groups. Any group from the syslog messages will be ignored. • *Remote users*: Users are defined on a remote LDAP server and user groups are retrieved from the LDAP server. Any group from the syslog messages will be ignored.

4. Select *OK* to add the source.

Predefined rules

Predefined matching rules are included for Cisco and Aruba wireless controllers.

Cisco ISE

Accounting Start Log

Trigger	`CISE_RADIUS_Accounting`
Auth Type Indicators	`Acct-Status-Type=Start` (Login)
Username field	`User-Name={{user}},`
Client IP field	`Framed-IP-Address={{ip}},`

Accounting Stop Log

Trigger	`CISE_RADIUS_Accounting`
Auth Type Indicators	`Acct-Status-Type=Stop` (Logout)
Username field	`User-Name={{user}},`
Client IP field	`Framed-IP-Address={{ip}},`

Aruba

Trigger	None; any logs are accepted.
Auth Type Indicators	`User Authentication Successful` (Login) (exact match required; no delimiter or value)
Username field	`username={{user}},`
Client IP field	`Framed-IP-Address={{ip}},`
Group field	`profile={{group}},`

FortiGate group filtering

If you are providing FSSO to only certain groups on a remote LDAP server, you can filter the polling information so that it includes only those groups, or organizational units (OU).

To view a list of the FortiGate group filters, go to *Fortinet SSO Methods* > *SSO* > *FortiGate Filtering*.

To create a new group filter:

1. From the FortiGate group filters select *Create New*.
   The *Create New FortiGate Group Filter* window opens.
2. Enter the following information:

Name	Enter a name in the *Name* field to identify the filter.
FortiGate name/IP	Enter the FortiGate unit's FQDN or IP address.
Description	Optionally, enter a description of the filter.

Forward FSSO information for users from the following subset of users/groups/containers/OUs only	Select to forward FSSO information for users from only the specific subset of users, groups, or containers. Select *Create New* under *SSO Filtering Objects*, enter a name to identify the policy, and select the object type: **Group:** Specifies the DN of a group. All users who are members of that group must be included in SSO. **Group container:** Specifies the DN of an LDAP container, e.g. OU. All users who are members of a group under that container or one of its sub-containers must be included in SSO. **User:** Specifies the DN of a user. This user must be included in SSO. **User container:** Specifies the DN of an LDAP container, e.g. OU. All users who are under that container or one of its sub-containers must be included in SSO. **User and group container:** Specifies the DN of an LDAP container, e.g. OU. It is the union of the user and the group containers. You can also use the *Import* option to import an existing object.
Enable IP filtering for this service	Select to enable IP filtering for this service. Choose the desired IP filtering rules from the *Available IP filtering rules* box and move them to the *Selected IP filtering rules* box. See IP filtering rules on page 1 for more information.

3. Select *OK* to create the new FortiGate group filter.

IP filtering rules

The user logon information that is sent to the FortiGate units can be restricted to specific IP addresses or address ranges. If no filters are defined, information is sent for all addresses.

To view the list of the IP filtering rules, go to *Fortinet SSO Methods* > *SSO* > *IP Filtering Rules*.

To create new IP filtering rules:

1. From the IP filtering rules list, select *Create New*. The *Create New IP Filtering Rule* window opens.
2. Enter the following information:

Name	Enter a name for the rule.
Filter Type	Select whether the rule will specify an IP address and netmask or an IP address range.
Rule	Enter either an IP address and netmask or an IP address range (depending on the selected filter type). For example: • IP/Mask: `10.0.0.1/255.255.255.0` • IP Range: `10.0.0.1/10.0.0.99`

3. Select *OK* to create the new IP filtering rule.

Tiered architecture

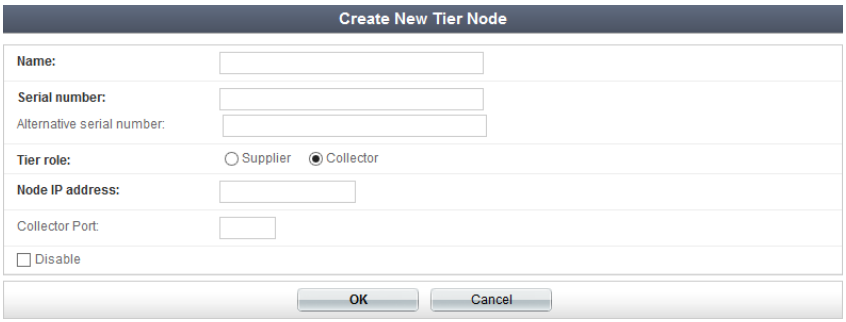
Tier nodes can be managed by going to *Fortinet SSO Methods* > *SSO* > *Tiered Architecture*.

The following options are available:

Create New	Select to create a new tier node.
Delete	Select to delete the selected node or nodes.
Edit	Select to edit the selected node.
Search	Enter a search term in the search text box then select *Search* to search the tier node list.
Name	The node name.
Tier Role	The node's tier role, either *Collector* or *Supplier*.
Address	The IP address of the node.
Port	The collector port number. Only applicable if *Tier Role* is *Collector*.
Serial Number	The serial number or numbers.
Enabled	If the node is enabled, a green circle with a check mark will be shown. A node can be disabled without losing any of its settings.

To add a new tier node:

1. From the tier node list, select *Create New*. The *Create New Tier Node* window opens.



2. Enter the following information:

Name	Enter a name to identify the node.
Serial number	Enter the device serial number.

Alternate serial number	Optionally, enter a second, or alternate, serial number for an HA cluster member.
Tier Role	Select the tier node role, either *Supplier* or *Collector*.
Node IP address	Enter the IP address for the supplier or collector.
Collector port	Enter the collector port number. Default is 8002. This only applies is *Collector* is selected as the *Tier Role*.
Disable	Disable the node without losing any of its settings.

3. Select *OK* to create the new tier node.

FortiClient SSO Mobility Agent

The FortiClient SSO Mobility Agent is a feature of FortiClient Endpoint Security. The agent automatically provides user name and IP address information to the FortiAuthenticator unit for transparent authentication. IP address changes, such as those due to WiFi roaming, are automatically sent to the FortiAuthenticator. When the user logs off or otherwise disconnects from the network, the FortiAuthenticator unit is aware of this and deauthenticates the user.

The *FortiClient SSO Mobility Agent Service* must be enabled. See Enable FortiClient SSO Mobility Agent Service on page 1.

For information on configuring FortiClient, see the *FortiClient Administration Guide* for your device.

Fake client protection

Some attacks are based on a user authenticating to an unauthorized AD server in order to spoof a legitimate user logon through the FortiClient SSO Mobility Agent. You can prevent this type of attack by enabling NTLM authentication (see Enable NTLM on page 1).

The FortiAuthenticator unit will initiate NTLM authentication with the client, proxying the communications only to the legitimate AD servers it is configured to use.

If NTLM is enabled, the FortiAuthenticator unit requires NTLM authentication when:

- the user logs on to a workstation for the first time,
- the user logs off and then logs on again,
- the workstation IP address changes,
- the workstation user changes,
- NTLM authentication expires (user configurable).

RADIUS Single Sign-On

A FortiGate or FortiMail unit can transparently identify users who have already authenticated on an external RADIUS server by parsing RADIUS accounting records. However, this approach has potential difficulties:

- The RADIUS server is business-critical IT infrastructure, limiting the changes that can be made to the server configuration.
- In some cases, the server can send accounting records only to a single endpoint. Some network topologies may require multiple endpoints.

The FortiAuthenticator RADIUS Accounting Proxy overcomes these limitations by proxying the RADIUS accounting records, modifying them, and replicating them to the multiple subscribing endpoints as needed.

RADIUS accounting proxy

The FortiAuthenticator receives RADIUS accounting packets from a carrier RADIUS server, transforms them, and then forwards them to multiple FortiGate or FortiMail devices for use in RADIUS Single Sign-On. This differs from the packet use of RADIUS accounting (RADIUS accounting on page 1).

The accounting proxy needs to know:

- Rule sets to define or derive the RADIUS attributes that the FortiGate unit requires,
- The source of the RADIUS accounting records: the RADIUS server,
- The destination(s) of the accounting records: the FortiGate units using this information for RADIUS SSO authentication.

General settings

General RADIUS accounting proxy settings can be configure by going to *Fortinet SSO Methods* > *Accounting Proxy* > *General*.

The following settings are available:

Log level	Select *Debug*, *Info*, *Warning*, or *Error* as the minimum severity level of event to log from the drop-down list.
Group cache lifetime	Enter the amount of time after which user group memberships will expire in the cache, from 1 to 10080 minutes (7 days). The default is 480 minutes.
Number of proxy retries	Enter the number of times to retry proxy requests if they timeout, from 0 to 3 retries, where 0 disables retries. The default is 3 retries.
Proxy retry timeout	Enter the retry period (timeout) of a proxy request, from 1 to 10 seconds.
Statistics update period	Enter the time between statistics updates to the seconds debug log, from 1 to 3600 seconds (1 hour).

Select *OK* to apply your changes.

Rule sets

A rule set can contain multiple rules. Each rule can do one of:

- add an attribute with a fixed value
- add an attribute retrieved from a user's record on an LDAP server
- rename an attribute to make it acceptable to the accounting proxy destination.

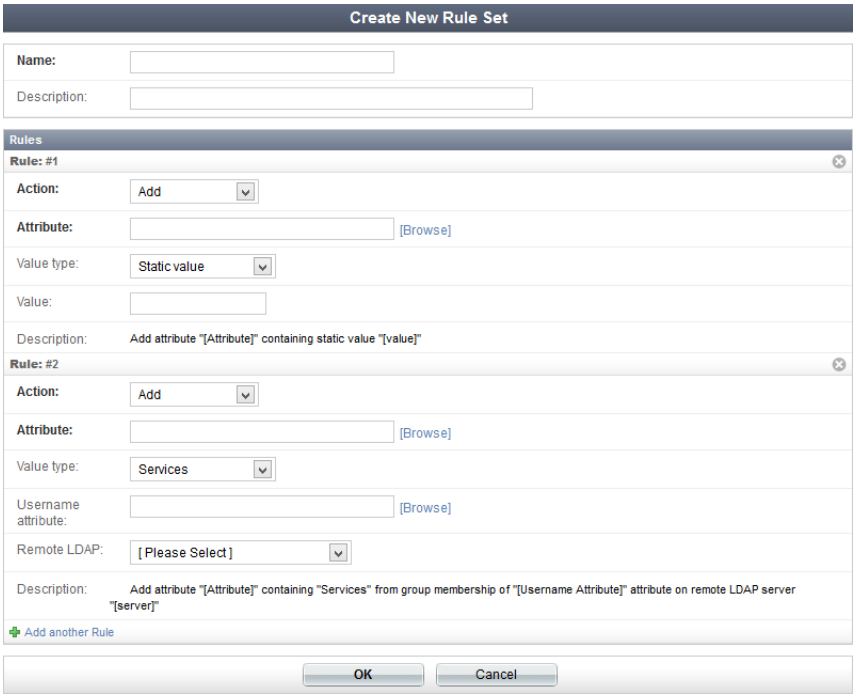
The FortiAuthenticator unit can store up to 10 rule sets. You can provide both a name and a description to each rule set to help you remember each rule set's purpose.

Rules access RADIUS attributes of which there are both standard attributes and vendor-specific attributes (VSAs). To select a standard attribute, select the Default vendor. See RADIUS attributes on page 1.

To view the accounting proxy rule set list, go to *Fortinet SSO Methods* > *Accounting Proxy* > *Rule Sets*.

To add RADIUS accounting proxy rule sets:

1. From the rule set list, select *Create New*. The *Create New Rule Set* window opens.



2. Enter the following information:

Name	Enter a name to use when selecting this rule set for an accounting proxy destination.
Description	Optionally, enter a brief description of the rule's purpose.
Rules	Enter one or more rules.

Action	The action for each rule can be either *Add* or *Modify*. • *Add*: add either a static value or a value derived from an LDAP server. • *Modify*: rename an attribute.
Attribute	Select *Browse* and choose the appropriate Vendor and Attribute ID in the *Select a RADIUS Attribute* dialog box.
Attribute 2	If the action is set to *Modify*, a second attribute may be selected. The first attribute will be renamed to the second attribute.
Value Type	If the action is set to *Add*, select a value type from the drop-down list. • *Static value*: adds the attribute in the *Attribute* field containing the static value in the *Value* field. • *Group names*: adds attribute in the *Attribute* field containing "Group names" from the group membership of the *Username Attribute* on the remote LDAP server. • *Services*: adds attribute in the *Attribute* field containing "Services" from the group membership of the *Username Attribute* on the remote LDAP server. • *UTM profile groups*: adds attribute in the *Attribute* field containing "UTM profile groups" from the group membership of the *Username Attribute* on the remote LDAP server.
Value	If the action is set to *Add* and *Value Type* is set to *Static value*, enter the static value.
Username Attribute	If the action is set to *Add,* and *Value Type* is not set to *Static value*, specify an attribute that provides the user's name, or select *Browse* and choose the appropriate Vendor and Attribute ID in the *Select a RADIUS Attribute* dialog box.
Remote LDAP	If the attribute addition requires an LDAP server, select one from the drop-down list. See LDAP on page 1 for information on remote LDAP servers.
Description	A brief description of the rule is provided.
Add another rule	Select to add another rule to the rule set.

3. Select *OK* to create the new rule set.

Example rule set

The incoming accounting packets contain the following fields:

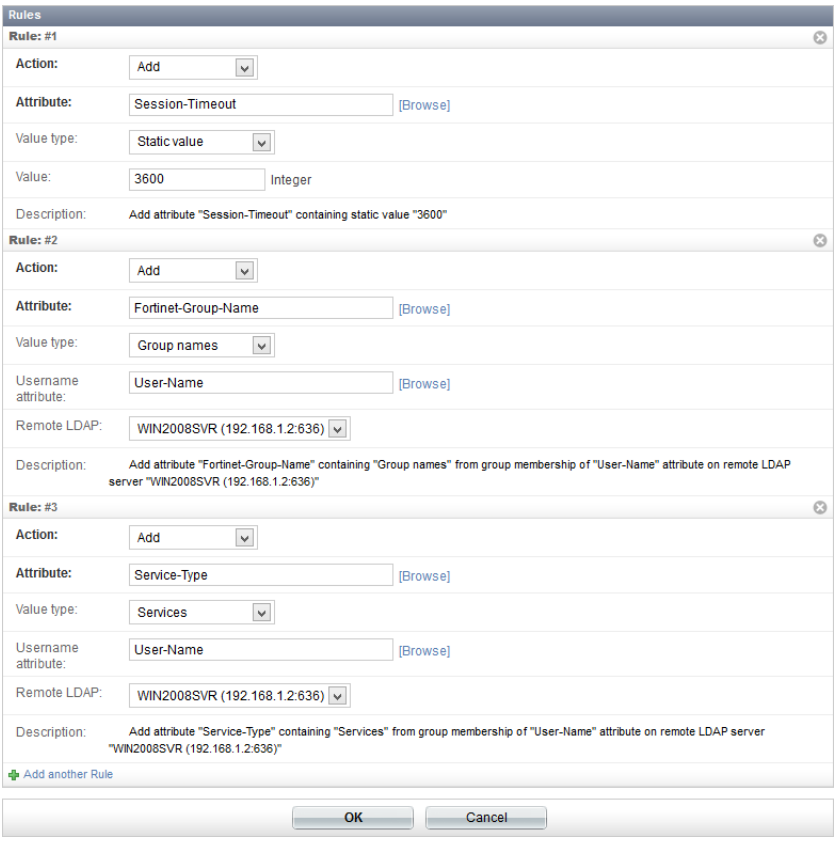
- User-Name
- NAS-IP-Address
- Fortinet-Client-IP-Address

The outgoing accounting packets need to have these fields:

- User-Name
- NAS-IP-Address

- Fortinet-Client-IP-Address
- Session-Timeout: Value is always 3600
- Fortinet-Group-Name: Value is obtained from user's group membership on remote LDAP
- Service-Type: Value is obtained from user's group membership and SSO Group Mapping

The rule set needs three rules to add Session-Timeout, Fortinet-Group-Name, and Service-Type. The following image provides an example:



Sources

The RADIUS accounting proxy sources list can be viewed in *Fortinet SSO Methods* > *Accounting Proxy* > *Sources*. Sources can be added, edited, and deleted as needed.

To add a RADIUS accounting proxy source:

1. From the source list, select *Create New*. The *Create New RADIUS Accounting Proxy Source* window opens.
2. Enter the following information:

Name	Enter the name of the RADIUS server. This is used in FortiAuthenticator configurations.
Source name/IP	Enter the FQDN or IP address of the server.
Secret	Enter the shared secret required to access the server.
Description	Optionally, enter a description of the source.

3. Select *OK* to add the RADIUS accounting proxy source.

Destinations

The destination of the RADIUS accounting records is the FortiGate unit that will use the records to identify users. When defining the destination, you also specify the source of the records (a RADIUS client already defined as a source) and the rule set to apply to the records.

To view the RADIUS accounting proxy destinations list, go to *Fortinet SSO Methods* > *Accounting Proxy* > *Destinations*.

To add a RADIUS accounting proxy destinations:

1. From the destinations list, select *Create New*. The *Create New RADIUS Accounting Proxy Destination* window opens.
2. Enter the following information:

Name	Enter a name to identify the destination device in your configuration.
Destination name/IP	Enter The FQDN or IP address of the FortiGate that will receive the RADIUS accounting records.
Secret	Enter the preshared key of the destination.
Source	Select a RADIUS client defined as a source from the drop-down list. See Sources on page 139.
Rule set	Select an appropriate rule set from the drop-down list or select *Create New* to create a new rule set. See Rule sets on page 137.

3. Select *OK* to add the RADIUS accounting proxy destination.

Monitoring

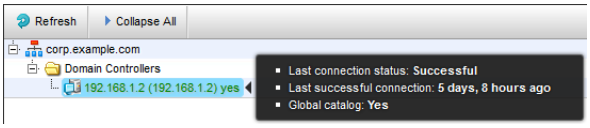
The *Monitor* menu tree provides options for monitoring SSO and authentication activity.

SSO

FortiAuthenticator can monitor the units that make up FSSO. This is useful to ensure there is a connection to the different components when troubleshooting.

Domains

To monitor SSO domains, go to *Monitor* > *SSO* > *Domains*. Select *Refresh* to refresh the domain list. Select *Expand All* to expand all of the listed domains, or *Collapse All* to collapse the view.



Hover the cursor over an entry to view additional information, such as the status and length of the last connection.

SSO Sessions

To monitor SSO sessions, go to *Monitor* > *SSO* > *SSO Sessions*. Users can be manually logged off of if required.

The following information is available:

Refresh	Refresh the SSO sessions list.
Logoff All	Log off all of the connected users.
Logoff Selected	Log off only the selected users.
Search	Enter a search term in the search field, then select *Search* to search the SSO sessions list.
Logon Time	When the session was started.
Update Time	When the session was last updated.
Workstation	The workstation that the user is using.
IP address	The IP address of the workstation.
Username	The username of the user.

Source	The source of the connection.
Group	The group to which the user belongs.

Domain Controllers

Domain controllers that are registered with the FortiAuthenticator unit can be viewed by going to *Monitor* > *SSO* > *Domain Controllers*.

The domain controllers list can be refreshed by selecting *Refresh*, and searched using the search field.

The list shows the connection status of the domain controller, as well as its update time and IP address. The total number of events, as well as the most recent event, are also shown.

FortiGates

FortiGate units that are registered with the FortiAuthenticator unit can be viewed at *Monitor* > *SSO* > *FortiGates*.

The list can be refreshed by selecting *Refresh* and searched using the search field. The list shows the connection time of each device, as well as its IP address and serial number.

User authentication events are logged in the FortiGate event log. See the *FortiGate Handbook* for more information.

DC/TS Agents

Domain Controller (DC) Agents and Terminal Server (TS) Agents that are registered with the FortiAuthenticator unit can be viewed at **Monitor > SSO > DC/TS Agents**.

The list can be refreshed by selecting **Refresh** and searched using the search field.

The list shows the server name of each agent, as well as its IP address, its agent type, last connection time, connection status, and the number of logged-on users.

Authentication

The Windows AD server and inactive users can be monitored from *Monitor* > *Authentication*. Learned RADIUS users can also be configured.

Locked-out Users

To view the locked out users, go to *Monitor* > *Authentication* > *Locked-out Users*.

Windows AD

As of FortiAuthenticator 4.2, FortiAuthenticator supports multiple Windows AD server forests, as shown below. A maximum of 20 Remote LDAP servers with Windows AD enabled can be configured at once. In addition, you can

now see when the server was updated last, and an option to reset the connection for individual servers.

To view the Windows AD server information, go to *Monitor* > *Authentication* > *Windows AD*.

Windows Active Directory Server #1	
Server name:	test
Primary IP Address:	10.10.10.10
Secondary IP address	None
Authentication Realm:	test
Agent:	running [Reset]
Connection:	connected
Updated:	49 seconds ago
Windows Active Directory Server #2	
Server name:	test2
Primary IP Address:	10.10.10.11
Secondary IP address	None
Authentication Realm:	test2
Agent:	running [Reset]
Connection:	connected
Updated:	73 seconds ago
Windows Active Directory Server #3	
Server name:	test3
Primary IP Address:	10.10.10.12
Secondary IP address	None
Authentication Realm:	test3
Agent:	running [Reset]
Connection:	connected
Updated:	49 seconds ago

To refresh the connection, select *Refresh* in the toolbar. The server name, IP address, authentication realm, agent, and connection are shown.

Windows device logins

To view the Windows device logins, go to *Monitor* > *Authentication* > *Windows Device Logins*.

To refresh the list, select *Refresh* in the toolbar. See Machine authentication on page 1 for more information.

Inactive users

To view a list of locked out, or inactive, users, go to *Monitor* > *Authentication* > *Inactive Users*.

To unlock a user from the list, select the user, then select *Unlock*. The list can be refreshed by selecting *Refresh*, and searched using the search field.

The list shows the username, server, the reason the user was locked out, and when they are locked out until.

For more information on locked out users, see Top User Lockouts widget on page 1, Lockouts on page 1, and User management on page 1.

Learned RADIUS users

Learned RADIUS users are users that have been learned by the FortiAuthenticator after they have authenticated against a remote RADIUS server.

For information on enabling learning RADIUS users, see RADIUS on page 1.

Certificate Management

This section describes managing certificates with the FortiAuthenticator device.

FortiAuthenticator can act as a CA for the creation and signing of X.509 certificates, such as server certificates for HTTPS and SSH, and client certificates for HTTPS, SSL, and IPSEC VPN.

The FortiAuthenticator unit has several roles that involve certificates:

Certificate authority	The administrator generates CA certificates that can validate the user certificates generated on this FortiAuthenticator unit. The administrator can import other authorities' CA certificates and Certificate Revocation Lists (CRLs), as well as generate, sign, and revoke user certificates. See End entities on page 1 for more information.
SCEP server	A SCEP client can retrieve any of the local CA certificates (Local CAs on page 1), and can have its own user certificate signed by the FortiAuthenticator unit CA.
Remote LDAP Authentication	Acting as an LDAP client, the FortiAuthenticator unit authenticates users against an external LDAP server. It verifies the identity of the external LDAP server by using a trusted CA certificate, see Trusted CAs on page 1.
EAP Authentication	The FortiAuthenticator unit checks that the client's certificate is signed by one of the configured authorized CA certificates, see Certificate authorities on page 1. The client certificate must also match one of the user certificates, see End entities on page 1.

Any changes made to certificates generate log entries that can be viewed at *Logging* > *Log Access* > *Logs*. See Logging on page 1.

This chapter includes the following sections:

- Policies
- End entities
- Certificate authorities
- SCEP

Policies

The policies section includes global configuration settings which are applied across all certificate authorities and end-entity certificates created on the FortiAuthenticator device.

Certificate expiry

Certificate expiration settings can be configured in *Certificate Management* > *Policies* > *Certificate Expiry*.

The following settings can be configured:

Warn when a certificate is about to expire	Enable sending a warning message to an administrator before a certificate expires.
Send a warning e-mail	Enter the number of days before the certificate expires that the email will be sent.
Administrator's e-mail	Enter the email address to which the expiry warning message will be sent.

Select *OK* to apply any configuration changes.

End entities

User and server certificates are required for mutual authentication on many HTTPS, SSL, and IPsec VPN network resources. You can create a user certificate on the FortiAuthenticator device, or import and sign a CSR. User certificates, client certificates, or local computer certificates are all the same type of certificate.

To view the user certificate list, go to *Certificate Management* > *End Entities* > *Users*. To view the server certificate list, go to *Certificate Management* > *End Entities* > *Local Services*.

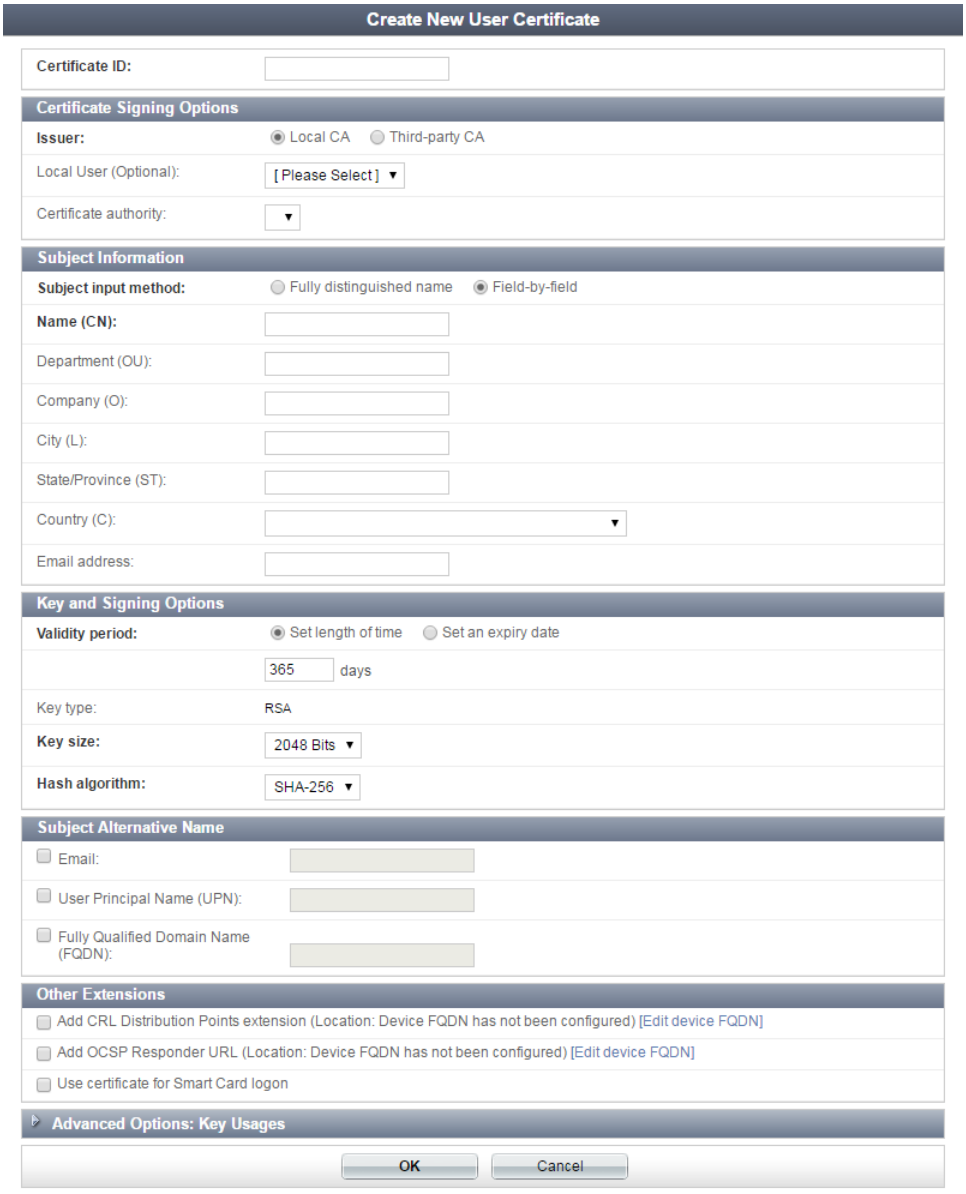
The following information is available:

Create New	Create a new certificate.
Import	Select to import a certificate signed by a third-party CA for a previously generated CSR (see To import a local user certificate: on page 151 and To import a server certificate: on page 151) or to import a CSR to sign (see To import a CSR to sign: on page 151).
Revoke	Revoke the selected certificate. See To revoke a certificate: on page 153.
Delete	Delete the selected certificate.
Export Certificate	Save the selected certificate to your computer.
Export PKCS#12	Export the PKCS#12. This is only available for user certificates.
Search	Enter a search term in the search field, then press Enter to search the certificate list.
Filter	Select to filter the displayed certificates by status. The available selections are: *All*, *Pending*, *Expired*, *Revoked*, and *Active*.
Certificate ID	The certificate ID.
Subject	The certificate's subject.
Issuer	The issuer of the certificate.
Status	The status of the certificate, either active, pending, or revoked.

Certificates can be created, imported, exported, revoked, and deleted as required. CSRs can be imported to sign, and the certificate detail information can also be viewed, see To view certificate details: on page 153.

To create a new certificate:

1. To create a new user certificate, go to *Certificate Management* > *End Entities* > *Users*. To create a new server certificate, go to *Certificate Management* > *End Entities* > *Local Services*.
2. Select *Create New* to open the *Create New User Certificate* or *Create New Server Certificate* window.



3. Configure the following settings:

Certificate ID	Enter a unique ID for the certificate.

Certificate Signing Options	
Issuer	Select the issuer of the certificate, either *Local CA* or *Third-party CA*. Selecting *Third-party CA* generates a CSR that is to be signed by a third-party CA.
Local User (Optional)	If *Local CA* is selected as the issuer, you may select a local user from the drop-down list to whom the certificate will apply. This option is only available when creating a new user certificate.
Certificate authority	If *Local CA* is selected as the issuer, select one of the available CAs configured on the FortiAuthenticator unit from the drop-down list. The CA must be valid and current. If it is not you will have to create or import a CA certificate before continuing. See Certificate authorities on page 1.
Subject Information	
Subject input method	Select the subject input method, either *Fully distinguished name* or *Field-by-field*.
Fully distinguished name	If the subject input method is *Fully distinguished name*, enter the full distinguished name of the subject. There should be no spaces between attributes.Valid DN attributes are DC, C, ST, L, O, OU, CN, and emailAddress. They are case-sensitive.
Field-by-field	If the subject input method is *Field-by-field*, enter the subject name in the *Name (CN)* field, and optionally enter the following fields: • *Department (OU)* • *Company (O)* • *City (L)* • *State/Province (ST)* • *Country (C)* (select from drop-down list) • *E-mail address*
Key and Signing Options	
Validity period	Select the amount of time before this certificate expires. This option is only available when *Issuer* is set to *Local CA*. Select *Set length of time* to enter a specific number of days, or select *Set an expiry date* and enter the specific date on which the certificate expires.
Key type	The key type is set to *RSA*.
Key size	Select the key size from the drop-down list: *1024*, *2048*, or *4096* bits.
Hash algorithm	Select the hash algorithm from the drop-down list, either *SHA-1* or *SHA-256*.

Subject Alternative Name	Subject Alternative Names (SAN) allow you to protect multiple host names with a single SSL certificate. SAN is part of the X.509 certificate standard. For example, SANs are used to protect multiple domain names such as www.example.com and www.example.net, in contrast to wildcard certificates that can only protect all first-level subdomains on one domain, such as *.example.com.
Email	Enter the email address of a user to map to this certificate.
User Principal Name (UPN)	Enter the UPN used to find the user's account in Microsoft Active Directory. This will map the certificate to this specific user. The UPN is unique for the Windows Server domain. This is a form of one-to-one mapping.
Fully Qualified Domain Name (FQDN)	Enter the FQDN to add OCSP URI extension. The resulting certificate will show this value as the subjectAltName attribute.
Other Extensions	This option is only available when creating a new user certificate, and when *Issuer* is set to *Local CA*.
Add CRL Distribution Points extension	Select to add CRL distribution points extension to the certificate. **Note:** Once a certificate is issued with this extension, the server must be able to handle the CRL request at the specified location. A DNS domain name must be configured. If it has not been, select *Edit DNS name* to configure one. See DNS on page 1.
Add OCSP Responder URL	Select to enable OCSP and add OCSP responder URL extension to the certificate. An FQDN must be configured. If it has not been, select *Edit device FQDN* to configure one.
Use certificate for Smart Card logon	Select to use the certificate for smart card logon.
Advanced Options: Key Usages	Some certificates require the explicit presence of key usage attributes before the certificate can be accepted for use.
Digital Signature	A high-integrity signature that assures the recipient that a message was not altered in transit
Non Repudiation	An authentication that is deemed as genuine with high assurance.
Key Encipherment	Uses the public key to encrypt private or secret keys.
Data Encipherment	Uses the public key to encrypt data.
Key Agreement	An interactive method for multiple parties to establish a cryptographic key, based on prior knowledge of a password.
Certificate Sign	A message from an applicant to a certificate authority in order to apply for a digital identity certificate.

CRL Sign	A Certificate Revocation List (CRL) Sign states a validity period for an issued certificate.
Encipher Only	Information will be converted into code only.
Decipher Only	Code will be converted into information only.
Advanced Options: Extended Key Usages	Some certificates require the explicit presence of *extended* key usage attributes before the certificate can be accepted for use.
Server Authentication	Authentication will only be granted when the user submits their credentials to the server.
Client Authentication	Authentication will be granted to the server by exchanging a client certificate.
Code Signing	Used to confirm the software author, and guarantees that the code has not been altered or corrupted through use of a cryptographic hash.
Secure Email	A secure email sent over SSL encryption.
OCSP Signing	Online Certificate Status Protocol (OCSP) Signing sends a request to the server for certificate status information. The server will send back a response of "current", "expired", or "unknown". OCSP permits a grace period to users or are expired, allowing them a limited time period to renew. This is usually used over CRL.
IPSec End System	
IPSec Tunnel Termination	IPSec SAs (Security Associations) are terminated through deletion or by timing out.
IPSec User	
IPSec IKE Intermediate (end entity)	An intermediate certificate is a subordinate certificate issued by a trusted root specifically to issue end-entity certificates. The result is a certificate chain that begins at the trusted root CA, through the intermediate CA (or CAs) and ending with the SSL certificate issued to you.
Time Stamping	
Microsoft Individual Code Signing	User submits information that is compared to an independent consumer database to validate their credentials.
Microsoft Commercial Code Signing	User submits information that proves their identity as corporate representatives.
Microsoft Trust List Signing	Uses a Certificate Trust List (CTL), a list of hashes of certificates. The list is comprised of pre-authenticated items that were approved by a trusted signing entity.
Microsoft/Netscape Server Gated Crypto	A defunct mechanism that stepped up 40-bit and 50-bit to 128-bit cipher suites with SSL.

	Microsoft Encrypted File System	The Encrypted File System (EFS) enables files to be transparently encrypted to protect confidential data.
	Microsoft EFS File Recovery	The certificate will be granted on the condition it has an EFS file recovery agent prepared.
	Smart Card Logon	The certificate will be granted on the condition that the user logs on to the network with a smart card.
	EAP over PPP/LAN	Extensible Authentication Protocol (EAP) will operate within either a Point-to-Point Protocol (PPP) or Local Area Network (LAN) framework
	KDC Authentication	An Authentication Server (AS) forwards usernames to a key distribution center (KDC), which issues an encrypted, time stamped ticket back to the user.

4. Select *OK* to create the new certificate.

To import a local user certificate:

1. Go to *Certificate Management* > *End Entities* > *Users* and select *Import*.
2. In the *Import Signing Request or Certificate* window, in the *Type* field, select *Local certificate*.
3. Select *Browse...* to locate the certificate file on your computer.
4. Select *OK* to import the certificate.

To import a server certificate:

1. to *Certificate Management* > *End Entities* > *Local Services* and select *Import*.
2. In the *Import Certificate* window, select *Browse...* to locate the certificate file on your computer.
3. Select *OK* to import the certificate.

To import a CSR to sign:

1. Go to *Certificate Management* > *End Entities* > *Users* and select *Import*.
2. In the *Import Signing Request or Certificate* window, in the *Type* field, select *CSR to sign*.

3. Configure the following settings:

Certificate ID	Enter a unique ID for the certificate.
CSR file (.csr, .req)	Select *Browse...* then locate the CSR file on your computer.
Certificate Signing Options	
Certificate authority	Select one of the available CAs configured on the FortiAuthenticator from the drop-down list. The CA must be valid and current. If it is not you will have to create or import a CA certificate before continuing. See Certificate authorities on page 1.
Validity period	Select the amount of time before this certificate expires. Select *Set length of time* to enter a specific number of days, or select *Set an expiry date* and enter the specific date on which the certificate expires
Hash algorithm	Select the hash algorithm from the drop-down list, either SHA-1 or SHA-256.
Subject Alternative Name	
Email	Enter the email address of a user to map to this certificate.
User Principal Name (UPN)	Enter the UPN used to find the user's account in Microsoft Active Directory. This will map the certificate to this specific user. The UPN is unique the Windows Server domain. This is a form of one-to-one mapping.
Other Extensions	

Add CRL Distribution Points extension	Select to add CRL distribution points extension to the certificate. **Note:** Once a certificate is issued with this extension, the server must be able to handle the CRL request at the specified location. A DNS domain name must be configured. If it has not been, select *Edit DNS name* to configure one. See DNS on page 1.
Use certificate for Smart Card logon	Select to use the certificate for smart card logon. This option can only be selected concurrently with *Add CRL Distribution Points extension*.

4. Select *OK* to import the CSR.

To revoke a certificate:

1. Go to *Certificate Management* > *End Entities* > *Users* or to *Certificate Management* > *End Entities* > *Local Services*.
2. Select the certificate the will be revoked, then select *Revoke*. The *Revoke User Certificate* or *Revoke Server Certificate* window opens.
3. Select a reason for revoking the certificate from the *Reason code* drop-down list. The reasons available are:
   - *Unspecified*
   - *Key has been compromised*
   - CA *has been compromised*
   - *Changes in affiliation*
   - *Superseded*
   - *Operation ceased*
   - *On Hold*

   Some of these reasons are security related (such as the key or CA being compromised), while others are more business related; a change in affiliation could be an employee leaving the company; *Operation ceased* could be a project that was cancelled.
4. Select *OK* to revoke the certificate.

To view certificate details:

From the certificate list, select a certificate ID to open the *Certificate Detail Information* window.

Select *Edit* next to the *Certificate ID* field to change the certificate ID. If any of this information is out of date or incorrect, you will not be able to use this certificate. If this is the case, delete the certificate and re-enter the information in a new certificate, see To create a new certificate: on page 147. Select *Close* to return to the certificate list.

Certificate authorities

A CA is used to sign other server and client certificates. Different CAs can be used for different domains or certificates. For example, if your organization is international you may have a CA for each country, or smaller organizations might have a different CA for each department. The benefits of multiple CAs include redundancy, in case there are problems with one of the well-known trusted authorities.

Once you have created a CA certificate, you can export it to your local computer.

Local CAs

The FortiAuthenticator device can act as a self-signed or local CA.

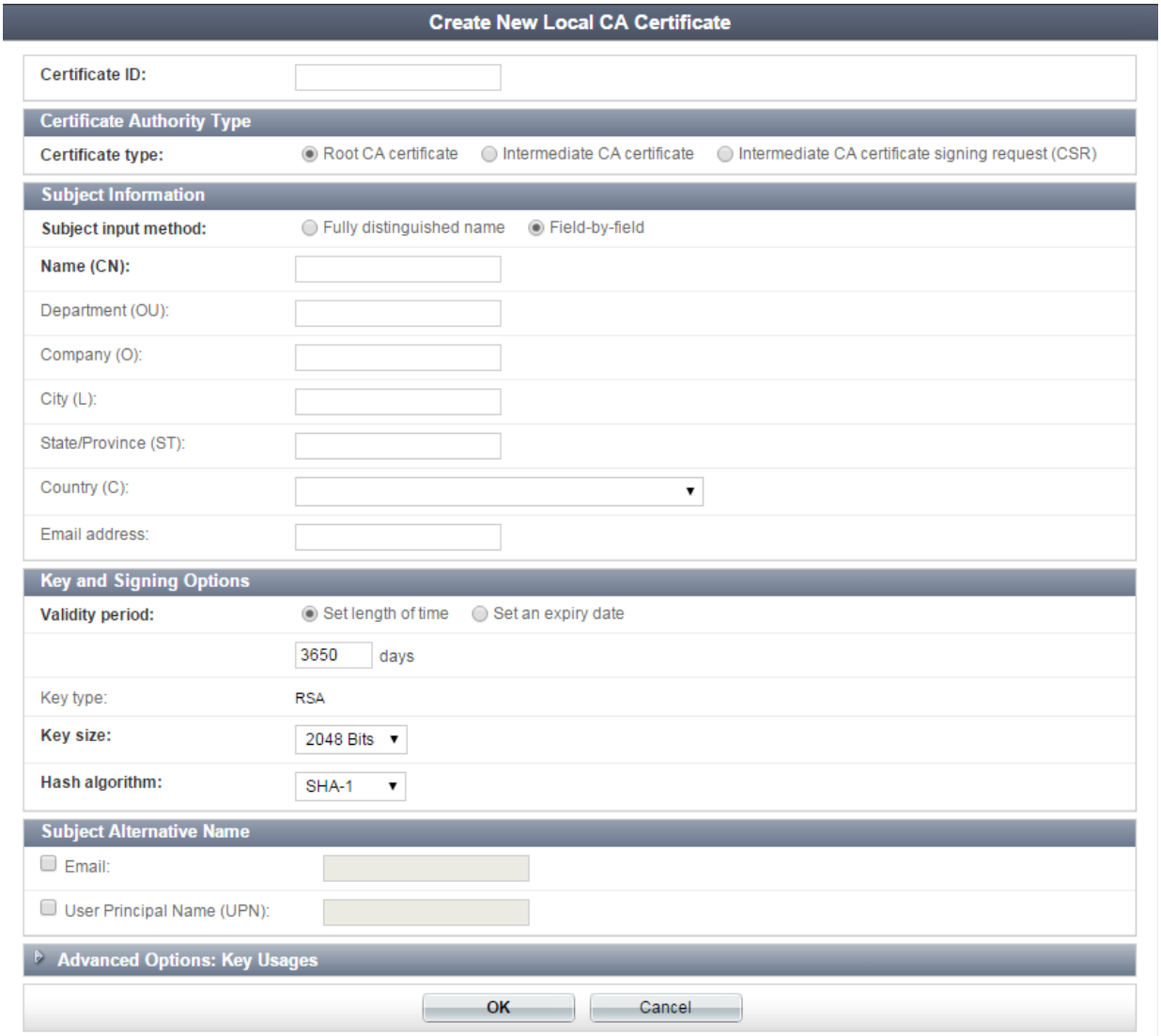
To view the certificate information, go to *Certificate Management* > *Certificate Authorities* > *Local CAs*.

The following information in shown:

Create New	Create a new CA certificate.
Import	Import a CA certificate. See Importing CA certificates and signing requests on page 158.
Revoke	Revoke the selected CA certificate.
Delete	Delete the selected CA certificate.
Export	Save the selected CA certificate to your computer.
Search	Enter a search term in the search field, then press Enter to search the CA certificate list. The search will return certificates that match either the subject or issuer.
Filter	Select to filter the displayed CAs by status. The available selections are: *All*, *Pending*, *Expired*, *Revoked*, and *Active*.
Certificate ID	The CA certificate ID.
Subject	The CA certificate subject.
Issuer	The issuer of the CA certificate.
Status	The status of the CA certificate, either active, pending, or revoked.
CA Type	The CA type of the CA certificate.

To create a CA certificate:

1. From the local CA certificate list, select *Create New*. The *Create New Local CA Certificate* window opens.



2. Enter the following information:

Certificate ID	Enter a unique ID for the CA certificate.
Certificate Authority Type	

Certificate type	Select one of the following options: • *Root CA certificate*: a self-signed CA certificate • *Intermediate CA certificate*: a CA certificate that refers to a different root CA as the authority • *Intermediate CA certificate signing request (CSR)*
Certificate authority	Select one of the available CAs from the drop-down list. This field is only available when the certificate type is *Intermediate CA certificate*.
Subject Information	
Subject input method	Select the subject input method, either *Fully distinguished name* or *Field-by-field*.
Fully distinguished name	If the subject input method is *Fully distinguished name*, enter the full distinguished name of the subject. There should be no spaces between attributes. Valid DN attributes are DC, C, ST, L, O, OU, CN, and emailAddress. They are case-sensitive.
Field-by-field	If the subject input method is *Field-by-field*, enter the subject name in the *Name (CN)* field, and optionally enter the following fields: • *Department (OU)* • *Company (O)* • *City (L)* • *State/Province (ST)* • *Country (C)* (select from drop-down list) • *E-mail address*
Key and Signing Options	
Validity period	Select the amount of time before this certificate expires. Select *Set length of time* to enter a specific number of days, or select *Set an expiry date* and enter the specific date on which the certificate expires. This option is not available when the certificate type is set to *Intermediate CA certificate signing request (CSR)*.
Key type	The key type is set to *RSA*.
Key size	Select the key size from the drop-down list: *1024*, *2048*, or *4096* bits.
Hash algorithm	Select the hash algorithm from the drop-down list, either *SHA-1* or *SHA-256*.
Subject Alternative Name	SANs allow you to protect multiple host names with a single SSL certificate. SAN is part of the X.509 certificate standard. This section is not available when the certificate type is *Intermediate CA certificate signing request (CSR)*.

	Email	Enter the email address of a user to map to this certificate.
	User Principal Name (UPN)	Enter the UPN used to find the user's account in Microsoft Active Directory. This will map the certificate to this specific user. The UPN is unique for the Windows Server domain. This is a form of one-to-one mapping.
Advanced Options: Key Usages		Some certificates require the explicit presence of extended key usage attributes before the certificate can be accepted for use.
	Key Usages	• Digital Signature • Non Repudiation • Key Encipherment • Data Encipherment • Key Agreement • Certificate Sign • CRL Sign • Encipher Only • Decipher Only
	Extended Key Usages	• Server Authentication • Client Authentication • Code Signing • Secure Email • OCSP Signing • IPSec End System • IPSec Tunnel Termination • IPSec User • IPSec IKE Intermediate (end entity) • Time Stamping • Microsoft Individual Code Signing • Microsoft Commercial Code Signing • Microsoft Trust List Signing • Microsoft Server Gated Crypto • Netscape Server Gated Crypto • Microsoft Encrypted File System • Microsoft EFS File Recovery • Smart Card Logon • EAP over PPP • EAP over LAN • KDC Authentication

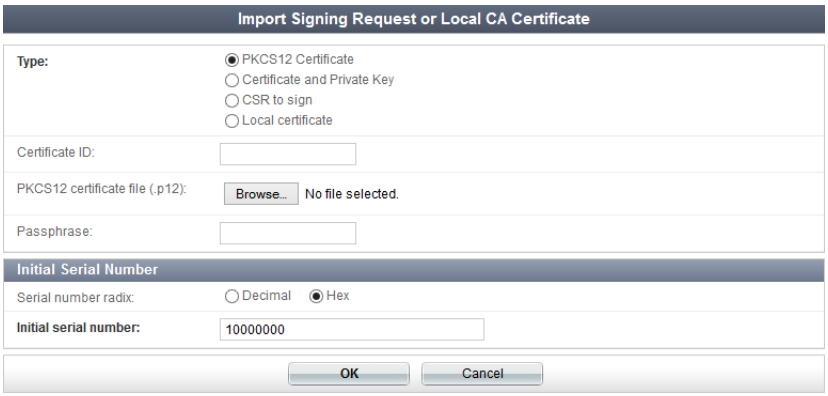
3. Select *OK* to create the new CA certificate.

Importing CA certificates and signing requests

Four options are available when importing a certificate or signing request: *PKCS12 Certificate*, *Certificate and Private Key*, *CSR to sign*, and *Local certificate*.

To import a PKCS12 certificate:

1. From the local CA certificate list, select *Import*. The *Import Signing Request or Local CA Certificate* window opens.
2. Select *PKCS12 Certificate* in the type field.



3. Enter the following:

Certificate ID	Enter a unique ID for the certificate.
PKCS12 certificate file (.p12)	Select *Browse...* to locate the certificate file on your computer.
Passphrase	Enter the certificate passphrase.
Initial serial number	Select the serial number radix, either decimal or hex, in the *Serial number radix* field, then enter the initial serial number in the *Initial serial number* field.

4. Select *OK* to import the certificate.

To import a certificate with a private key:

1. From the local CA certificate list, select *Import*. The *Import Signing Request or Local CA Certificate* window opens.
2. Select *Certificate and Private Key* in the type field.
3. Enter the following:

Certificate ID	Enter a unique ID for the certificate.
Certificate file (.cer)	Select *Browse...* to locate the certificate file on your computer.
Private key file	Select *Browse...* to locate the private key file on your computer.

Passphrase	Enter the certificate passphrase.
Initial serial number	Select the serial number radix, either decimal or hex, in the *Serial number radix* field, then enter the initial serial number in the *Initial serial number* field.

4. Select *OK* to import the certificate.

To import a CSR to sign:

1. From the local CA certificate list, select *Import*. The *Import Signing Request or Local CA Certificate* window opens.
2. Select *CSR to sign* in the type field.
3. Enter the following:

Certificate ID	Enter a unique ID for the certificate.
CSR file (.csr, .req)	Select *Browse...* to locate the CSR file on your computer.
Certificate Signing Options	
Certificate authority	Select one of the available CAs from the drop-down list.
Validity period	Select the amount of time before this certificate expires. Select *Set length of time* to enter a specific number of days, or select *Set an expiry date* and enter the specific date on which the certificate expires.
Hash algorithm	Select the hash algorithm from the drop-down list, either SHA-1 or SHA-256.
Subject Alternative Name	This section is not available is the certificate type is *Intermediate CA certificate signing request (CSR)*.
Email	Enter the email address of a user to map to this certificate.
User Principal Name (UPN)	Enter the UPN used to find the user's account in Microsoft Active Directory. This will map the certificate to this specific user. The UPN is unique for the Windows Server domain. This is a form of one-to-one mapping.

4. Select *OK* to import the CSR.

To import a local CA certificate:

1. From the local CA certificate list, select *Import*. The *Import Signing Request or Local CA Certificate* window opens.
2. Select *Local certificate* in the type field.
3. Select *Browse...* in the *Certificate file (.cer)* field to locate the certificate file on your computer.
4. Select *OK* to import the local CA certificate.

CRLs

A CRL is a file that contains a list of revoked certificates, their serial numbers, and their revocation dates. The file also contains the name of the issuer of the CRL, the effective date, and the next update date. By default, the shortest validity period of a CRL is one hour.

Some potential reasons for certificates to be revoked include:

- A CA server was hacked and its certificates are no longer trustworthy,
- A single certificate was compromised and is no longer trustworthy,
- A certificate has expired and is not supposed to be used past its lifetime.

Go to *Certificate Management* > *Certificate Authorities* > *CRLs* to view the CRL list.

The following information is shown:

Import	Import a CRL.
Export	Save the selected CRL to your computer.
CA Type	The CA type of CRL.
Issuer name	The name of the issuer of the CRL.
Subject	The CRL's subject.
Revoked Certifications	The number of revoked certificates in the CRL.

To import a CRL:

1. Download the most recent CRL from a CDP. One or more CDPs are usually listed in a certificate under the Details tab.
2. From the CRL list, select *Import*.
3. Select *Browse...* to locate the file on your computer, then select *OK* to import the list.

   When successful, the CRL will be displayed in the CRL list on the FortiAuthenticator device. You can select it to see the details (see To view certificate details: on page 1).

Locally created CRLs

When you import a CRL, it is from another authority. If you are creating your own CA certificates, then you can also create your own CRL to accompany them.

As a CA, you sign user certificates. If for any reason you need to revoke one of those certificates, it will go on a local CRL. When this happens you need to export the CRL to all your certificate users so they are aware of the revoked certificate.

To create a local CRL:

1. Create a local CA certificate. See Local CAs on page 154.
2. Create one or more user certificates. See End entities on page 1.

3. Go to *Certificate Management* > *End Entities* > *Users*, select one or more certificates, and then select *Revoke*. See To revoke a certificate: on page 1.

   The selected certificates will be removed from the user certificate list and a CRL will be created with those certificates as entries in the list. If there is already a CRL for the CA that signed the user certificates, the certificates will be added to the current CRL.

If, at a later date, one or more CAs are deleted, their corresponding CRLs will also be deleted, along with any user certificates that they signed.

Configuring online certificate status protocol

FortiAuthenticator also supports Online Certificate Status Protocol (OCSP), defined in RFC 2560. To use OCSP, configure the FortiGate unit to use TCP port 2560 on the FortiAuthenticator IP address.

For example, configuring OCSP in FortiGate CLI for a FortiAuthenticator with an IP address of 172.20.120.16, looks like this:

```
config vpn certificate ocsp-server
   edit fac_ocsp
      set cert "REMOTE_Cert_1"
      set url "http://172.20.120.16:2560"
   end
```

Trusted CAs

Trusted CA certificates can be used to validate certificates signed by an external CA.

To view the trusted CA certificate list, go to *Certificate Management* > *Certificate Authorities* > *Trusted CAs*.

The certificate ID, subject, issuer, and status are shown. Certificates can be imported, exported, deleted, and searched.

To import a trusted CA certificate:

1. From the trusted CA certificate list, select *Import*. The *Import Signing Request or Trusted CA Certificate* window opens.
2. Enter a certificate ID in the *Certificate ID* field.
3. In the *Certificate* field, Select *Browse...* to locate the file on your computer, then select *OK* to import the list.

   When successful, the trusted CA certificate will be displayed in the list on the FortiAuthenticator device. You can select it to see the details (see To view certificate details: on page 1).

SCEP

The FortiAuthenticator device contains a SCEP server that can sign user CSRs, and distribute CRLs and CA certificates. To use SCEP, you must:

- Enable HTTP administrative access on the interface connected to the Internet. See Interfaces on page 1.
- Add the CA certificate for your certificate authority. See Certificate authorities on page 1.
- Select the CA to use for SCEP. See Default CA on page 162.

Users can request a user certificate through online SCEP, found at `http://<FortiAuthenticator IP Address>/cert/scep`.

General

As administrator, you can allow the FortiAuthenticator unit to either automatically sign the user's certificate or alert you about the request for signature.

To enable SCEP and configure general settings, go to *Certificate Management* > *SCEP* > *General*.

The following settings can be configured:

Enable SCEP	Select to enable SCEP.
Default CA	Select the default CA to use from the drop-down list.
Enrollment method	Select the enrollment method: • *Automatic*: The certificate is pre-approved by the administrator. The administrator enters the certificate information on the FortiAuthenticator unit and gives the user a challenger password to use when submitting their request. • *Manual and Automatic*: The user submits the CSR, the request shows up as pending on FortiAuthenticator unit, then the administrator manually approves the pending request. Optionally, enter an email address to send pending approval notifications to.
Default enrollment password	Enter the default enrollment password that will be used when not setting a random password.

Select *OK* to apply any changes you have made.

Enrollment requests

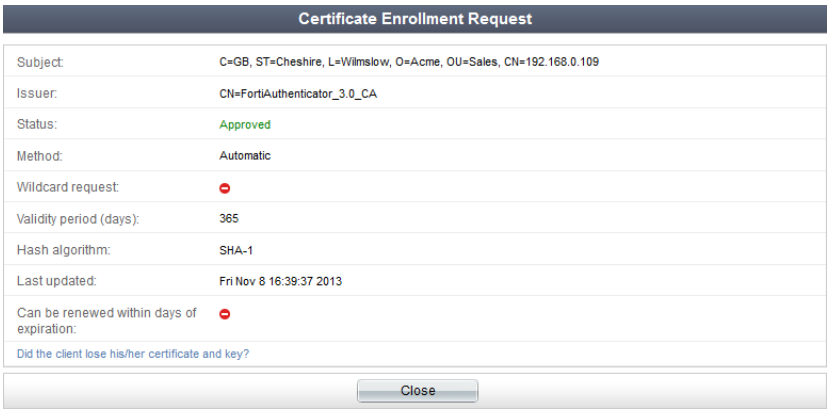
To view and manage certificate enrollment requests, go to *Certificate Management* > *SCEP* > *Enrollment Requests*.

The following information is available:

Create New	Create a new certificate enrollment request.
Delete	Delete the selected certificate enrollment request.
Approve/Reject	Approve or reject the selected certificate enrollment request.
Method	The enrollment method used.
Status	The status of the enrollment: pending, approved, or rejected.
Wildcard	If it is a wildcard request, a green circle with a check mark is shown.
Issuer	The issuer of the certificate.
Subject	The certificate subject.
Renewable Before Expiry (days)	The number of days before the certificate enrollment request expires that it can be renewed.
Updated at	The date and time that the enrollment request was last updated.

To view the enrollment request details:

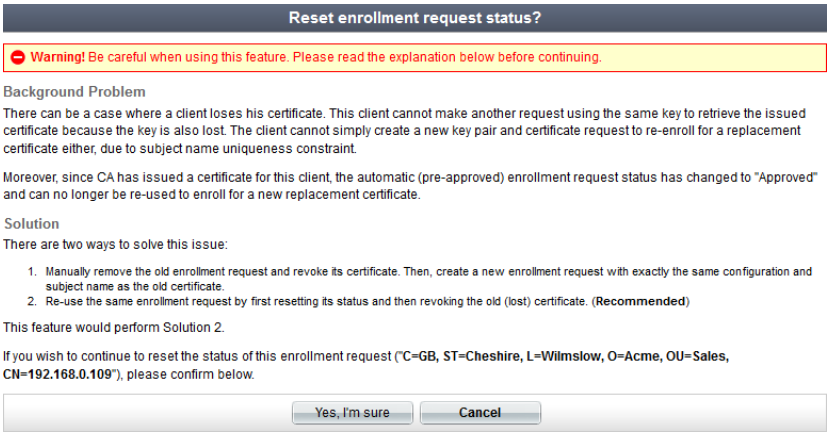
1. From the enrollment request list, select a request by clicking within its row. The *Certificate Enrollment Request* window opens.



2. If the client has lost their certificate and key, select *Did the client lose his/her certificate and key?*
3. Select *Close* to return to the enrollment request window.

To reset the enrollment request status:

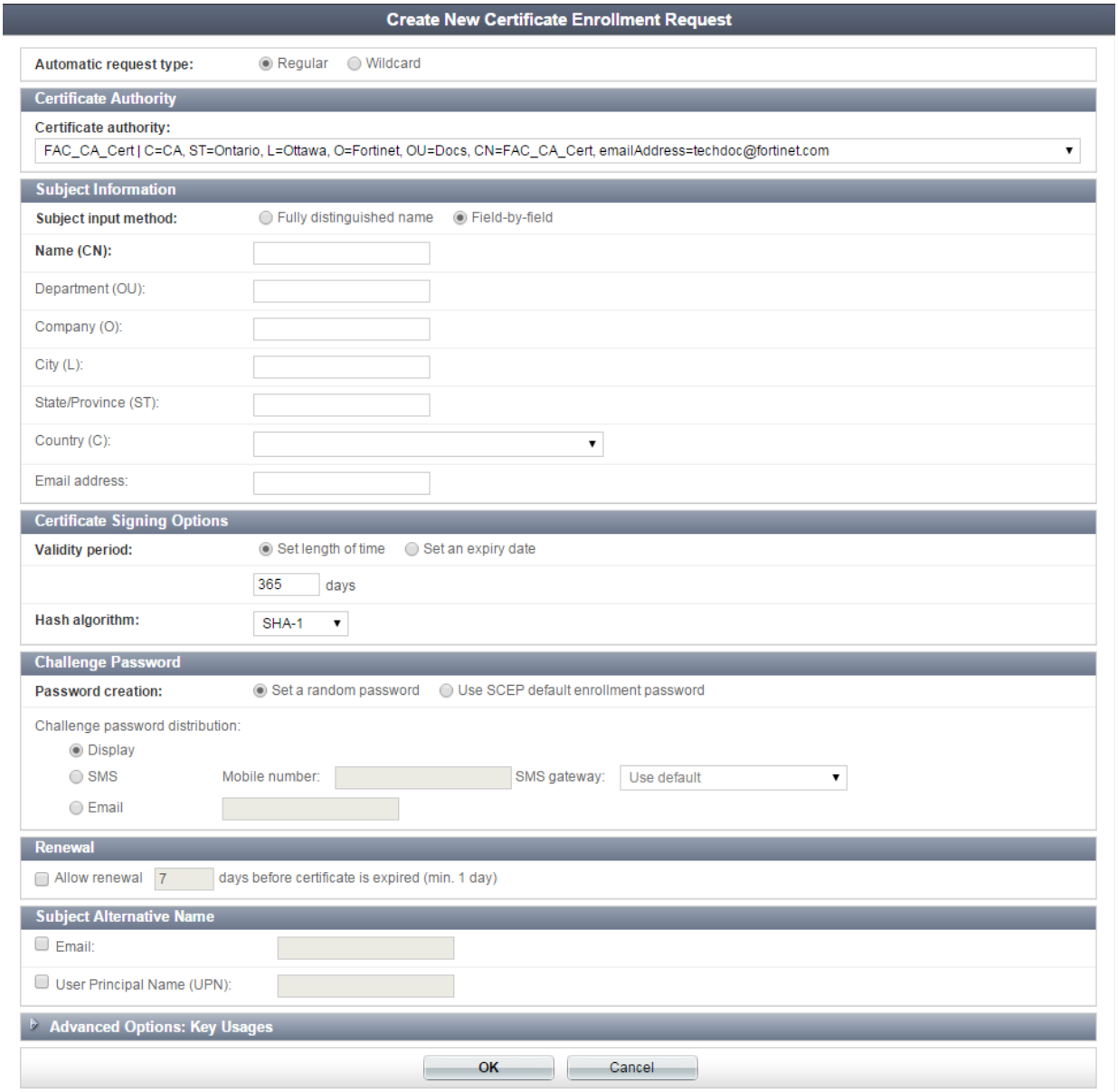
1. From the *Certificate Enrollment Request* window, select *Did the client lose his/her certificate and key?* The *Reset enrollment request status?* window opens.



2. There are two methods to reset the enrollment request:
   - Manually remove the old enrollment request, revoke its certificate, then create a new enrollment request with exactly the same configuration and subject name as the old certificate.
   - Re-use the same enrollment request by resetting its status and then revoking the lost certificate.
3. To re-use the same enrollment request, select *Yes, I'm sure*. This is the recommended method of resolving the issue.

To create a new certificate enrollment request:

1. From the certificate enrollment requests list, select *Create New*. The *Create New Certificate Enrollment Request* window opens.



2. Enter the following information:

Automatic request type	Select the automatic request type, either *Regular* or *Wildcard*.
Certificate Authority	Select one of the available CAs configured on the FortiAuthenticator unit from the drop-down list. The CA must be valid and current. If it is not you will have to create or import a CA certificate before continuing. See Certificate authorities on page 1.

Subject Information	
Subject input method	Select the subject input method, either *Fully distinguished name* or *Field-by-field*.
Fully distinguished name	If the subject input method is *Fully distinguished name*, enter the full distinguished name of the subject. There should be no spaces between attributes. Valid DN attributes are DC, C, ST, L, O, OU, CN, and emailAddress. They are case-sensitive.
Field-by-field	If the subject input method is *Field-by-field*, enter the subject name in the *Name (CN)* field (if the *Automatic request type* is set to *Regular*), and optionally enter the following fields: • *Department (OU)* • *Company (O)* • *City (L)* • *State/Province (ST)* • *Country (C)* (select from drop-down list) • *E-mail address*
Certificate Signing Options	
Validity period	Select the amount of time before this certificate expires. Select *Set length of time* to enter a specific number of days, or select *Set an expiry date* and enter the specific date on which the certificate expires.
Hash algorrithm	Select the hash algorithm from the drop-down list, either *SHA-1* or *SHA-256*.
Challenge Password	
Password creation	Select to either set a random password, or use the default enrollment password (see Default enrollment password on page 162).
Challenge password distribution	Select the challenge password distribution method. This option is only available if *Password creation* is set to *Set a random password*. • *Display*: display the password on the screen. • *SMS*: send the password to a mobile phone. Enter the phone number in the *Mobile number* field and select an SMS gateway from the drop-down list. • *E-mail*: send the password to the email address entered in the email field.
Renewal	To allow renewals, select *Allow renewal*, then enter the number of days before the certificate expires.
Subject Alternative Name	This option is only available if the *Automatic request type* is set to *Regular*.
Email	Enter the email address of a user to map to this certificate.

	User Principal Name (UPN)	**Enter the UPN used to find the user's account in Microsoft Active Directory. This will map the certificate to this specific user. The UPN is unique for the Windows Server domain. This is a form of one-to-one mapping.**
Advanced Options: Key Usages		**Some certificates require the explicit presence of extended key usage attributes before the certificate can be accepted for use.**
	Key Usages	• Digital Signature • Non Repudiation • Key Encipherment • Data Encipherment • Key Agreement • Certificate Sign • CRL Sign • Encipher Only • Decipher Only
	Extended Key Usages	• Server Authentication • Client Authentication • Code Signing • Secure Email • OCSP Signing • IPSec End System • IPSec Tunnel Termination • IPSec User • IPSec IKE Intermediate (end entity) • Time Stamping • Microsoft Individual Code Signing • Microsoft Commercial Code Signing • Microsoft Trust List Signing • Microsoft Server Gated Crypto • Netscape Server Gated Crypto • Microsoft Encrypted File System • Microsoft EFS File Recovery • Smart Card Logon • EAP over PPP • EAP over LAN • KDC Authentication

3. Select *OK* to create the new certificate enrollment request.

Logging

Accounting is an important part of FortiAuthenticator. The *Logging* menu tree provides a record of the events that have taken place on the FortiAuthenticator unit.

Log Access

To view the log events table, go to *Logging* > *Log Access* > *Logs*.

The following options and information are available:

Refresh	Refresh the log list.
Download Raw Log	Export the FortiAuthenticator log to your computer as a text file named *fac.log*.
Log Type Reference	Select to view the log type reference dialog box. See Log type reference on page 169.
Debug Report	Select to download the debug report to your computer as a file named *report.dbg*.
Search	Enter a search term in the search field, then select *Search* to search the log message list. The search string must appear in the Message portion of the log entry to result in a match. To prevent each term in a phrase from being matched separately, multiple keywords must be in quotes and be an exact match. After the search is complete the number of positive matches will be displayed next to the Search button, with the total number of log entries in brackets following. Select the total number of log entries to return to the full list. Subsequent searches will search all the log entries, and not just the previous search's results.
ID	The log message's ID.
Timestamp	The time the message was received.

Level	The log severity level: • *Emergency*: The system has become unstable. • *Alert*: Immediate action is required. • *Critical*: Functionality is affected. • *Error*: An erroneous condition exists, and functionality is probably affected. • *Warning*: Functionality could be affected. • *Notification*: Information about normal events. • *Information*: General information about system operations. • *Debug*: Detailed information useful for debugging purposes.
Category	The log category, which is always *Event*. See Log type reference on page 169.
Sub category	The log subcategory. See Log type reference on page 169.
Type id	The log type ID.
Action	The action which created the log message, if applicable.
Status	The status of the action that created the log message, if applicable.
NAS name/IP	The NAS name or IP address of the relevant device if an authentication action fails.
Short message	The log message itself, sometimes slightly shortened.
User	The user to whom the log message pertains.

To view log details:

From the log list, select the log whose details you need to view by clicking anywhere within the log's row. The *Log Details* pane will open on the right side of the window.

After viewing the log details, select the close icon in the top right corner of the pane to close the details pane.

Log type reference

Select *Log Type Reference* in the log list toolbar to open the log type reference dialog box.

The following information and options are available:

Search	Enter a search term in the search field, then select *Search* to search the log type reference.
Type id	The log type ID.
>Name	The name of the log type.

Sub category	The log type subcategory, one of: *Admin Configuration*, *Authentication*, *System*, *High Availability*, *User Portal*, or *Web Service*.
Category	The log type category, which is always *Event*.
Description	A brief description of the log type.

To close the *Log Type Reference* dialog box, select *close* above the top right corner of the box, or simply click anywhere outside of the box within the log list.

Sort the log messages

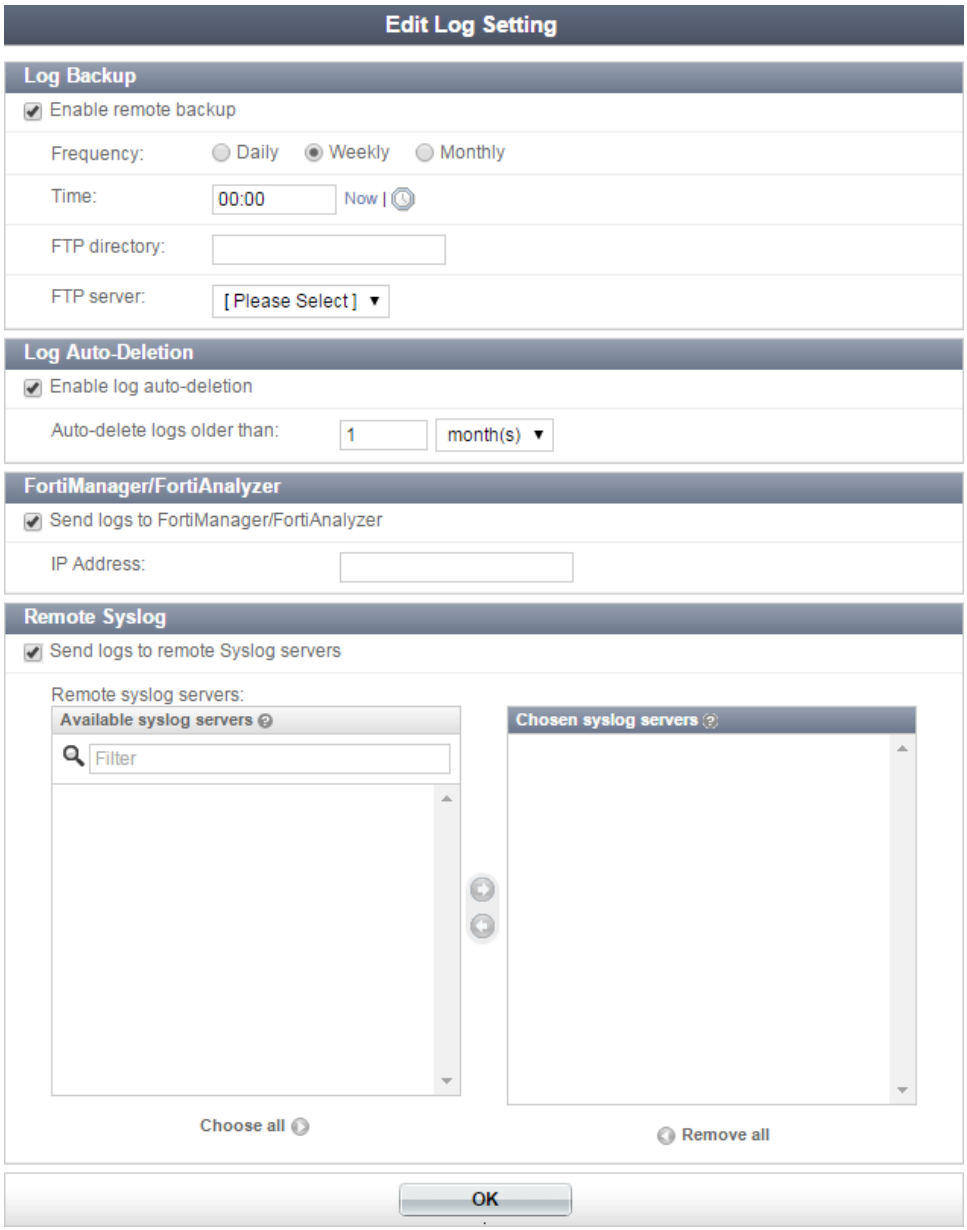
The log message table can be sorted by any column. To sort the log entries by a particular column, select the title for that column. The log entries will now be displayed based on data in that column in ascending order. Select the column heading again to sort the entries in descending order. Ascending or descending is displayed with an arrow next to the column title, an up arrow for ascending and down arrow for descending.

Log Configuration

Logs can be remotely backed up to an FTP server, automatically deleted, and sent to a remote syslog server in lieu of storing them locally.

Log Settings

To configure log backups, automatic deletion, and remote storage, go to *Logging* > *Log Config* > *Log Settings*.



To configure log backups:

1. In the log settings window, select *Enable remote backup* in the *Log Backup* section.
2. Select the frequency of the backups in the *Frequency* field as either *Daily*, *Weekly*, or *Monthly*.
3. Configure the time of day that the backup will occur in one of the following ways:
   - Enter a time in the *Time* field
   - Select *Now* to enter the current time
   - Select the clock icon and choose a time from the pop-up menu: *Now*, *Midnight*, *6 a.m.*, or *Noon*.
4. Select an FTP server from the drop-down list in the *FTP server* field. For information on configuring an FTP server, see FTP servers on page 1.
5. Select *OK* to save your settings.

To configure automatic log deletion:

1. In the log settings window, select *Enable log auto-deletion* in the *Log Auto-Deletion* section.
2. In the *Auto-delete logs older than* field, select *day(s)*, *week(s)*, or *month(s)* from the drop-down list, then enter the number of days, weeks, or months after which a log will be deleted.
3. Select *OK* to save your settings.

To configure logging to a FortiManager/FortiAnalyzer unit:

1. In the log settings window, select *Send logs to FortiManager/FortiAnalyzer* in the *FortiManager/FortiAnalyzer* section.
2. In the *IP Address* field, enter the Internet-facing IP address of the FortiManager or FortiAnalyzer unit.

FortiAnalyzer officially supports this feature in FortiAnalyzer 5.4.2 build 1117.

To configure logging to a remote syslog server:

1. In the log settings window, select *Send logs to remote Syslog servers* in the *Remote Syslog* section.
2. Move the syslog servers to which the logs will be sent from the *Available syslog servers* box to the *Chosen syslog servers* box.
   For information on adding syslog servers, see Syslog Servers on page 173.
3. Select *OK* to save your settings.

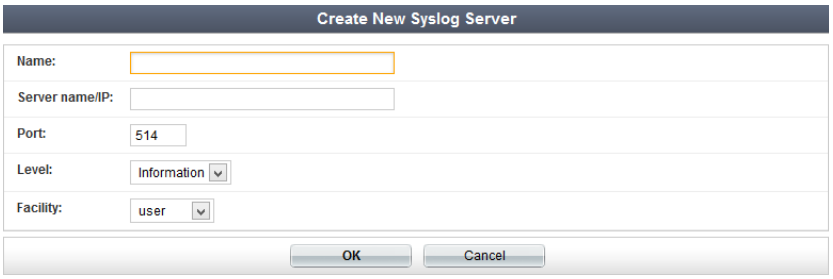
Syslog Servers

Syslog servers can be used to store remote logs. To view the syslog server list, go to *Logging* > *Log Config* > *Syslog Servers*.

Create New	Add a new syslog server.
Delete	Delete the selected syslog server or servers.
Edit	Edit the selected syslog server.
Name	The syslog server name on the FortiAuthenticator unit.
Server name/IP	The server name or IP address, and port number.

To add a syslog server:

1. From the syslog servers list, select *Create New*. The *Create New Syslog Server* window opens.



2. Enter the following information:

Name	Enter a name for the syslog server on the FortiAuthenticator unit.
Server name/IP	Enter the syslog server name or IP address.
Port	Enter the syslog server port number. The default port is 514.
Level	Select a log level to store on the remote server from the drop-down list. See Level on page 1.
Facility	Select a facility from the drop-down list.

3. Select *OK* to add the syslog server.

Troubleshooting

This chapter provides suggestions to resolve common problems encountered while configuring and using your FortiAuthenticator device, as well as information on viewing debug logs.

For more support, contact Fortinet Customer Service & Support (support.fortinet.com).

Before starting, please ensure that your FortiAuthenticator device is plugged in to an appropriate, and functional, power source.

Troubleshooting

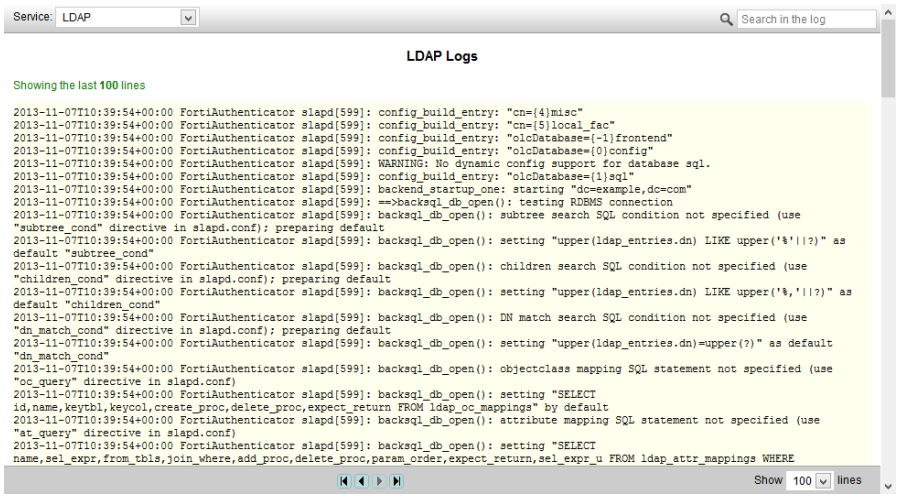
The following table describes some of the basic issues that can occur while using your FortiAuthenticator device, and suggestions on how to solve said issues.

Problem	Suggestions
All user log in attempts fail, there is no response from the FortiAuthenticator device, and there are no entries in the system log.	• Check that the authentication client has been correctly configured. See Adding a FortiAuthenticator unit to your network on page 1. • If the authentication client is not configured, all requests are silently dropped. • Verify that traffic is reaching the FortiAuthenticator device. • Is there an intervening Firewall blocking 1812/UDP RADIUS Authentication traffic, is the routing correct, is the authentication client configured with correct IP address for the FortiAuthenticator unit, etc.
All user log in attempts fail with the message *RADIUS ACCESS-REJECT*, and *invalid password* shown in the logs.	• Verify that the authentication client secrets are identical to those on the FortiAuthenticator unit.
Generally, user log in attempts are successful, however, an individual user authentication attempt fails with *invalid password* shown in the logs.	• Reset the user's password and try again. See Editing a user on page 1. • Have the user privately show their password to the administrator to check for unexpected characters (possibly due to keyboard regionalization issues).

Problem	Suggestions
Generally, user log in attempts are successful, however, an individual user authentication attempt fails with *invalid token* shown in the logs.	• Verify that the user is not trying to use a previously used PIN. • Tokens are One Time Passwords, so you cannot log in twice with the same PIN. • Verify that the time and timezone on the FortiAuthenticator unit are correct and, preferably, synchronised using NTP. See Configuring the system time, time zone, and date on page 1. • Verify that the token is correctly synchronized with the FortiAuthenticator unit, and verify the drift by synchronizing the token. See FortiToken drift adjustment on page 1. • Verify the user is using the token assigned to them (validate the serial number against the FortiAuthenticator unit configuration). See User management on page 1. • If the user is using an e-mail or SMS token, verify it is being used within the valid timeout period. See Lockouts on page 1.

Debug logs

Extended debug logs can be accessed by using your web browser to browse to `https://<FortiAuthenticator IP Address>/debug`.

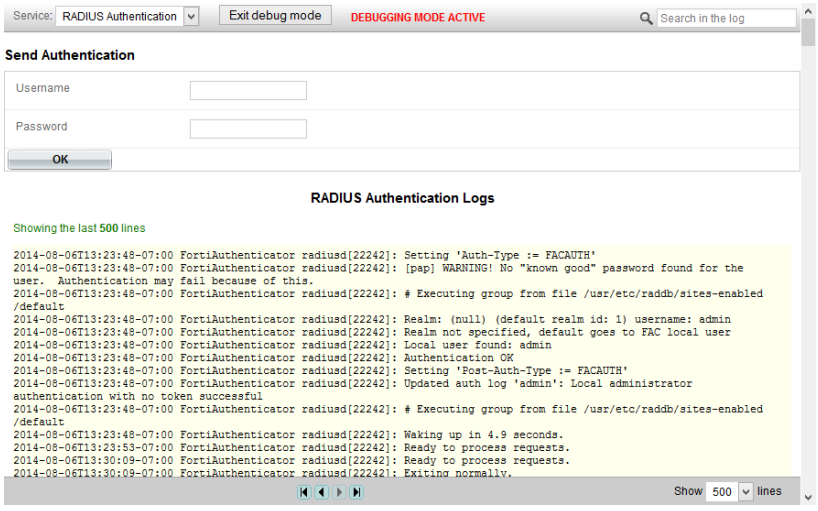


Service	Select the service whose logs are shown from the drop-down list: • FSSO Agent • GUI • HA • LDAP • RADIUS Accounting • RADIUS Authentication • SNMP • Startup • Web Server
Enter debug mode	If RADIUS Authentication is selected as the service, the option to enter the debug mode is available. See RADIUS debugging on page 177.
Search	Enter a search term in the search field, then select *Search* to search the debug logs.
Page navigation	Use the *First Page*, *Previous Page*, *Next Page*, and *Last Page* icons to navigated through the logs.
Show	Select the number of lines to show per page from the drop-down list. The options are: *100* (default), *250*, and *500*.

RADIUS debugging

RADIUS authentication debugging mode can be accessed to debug RADIUS authentication issues.

In the debug logs screen, select *RADIUS Authentication* from the *Service* drop-down list, then select *Enter debug mode* from the toolbar.



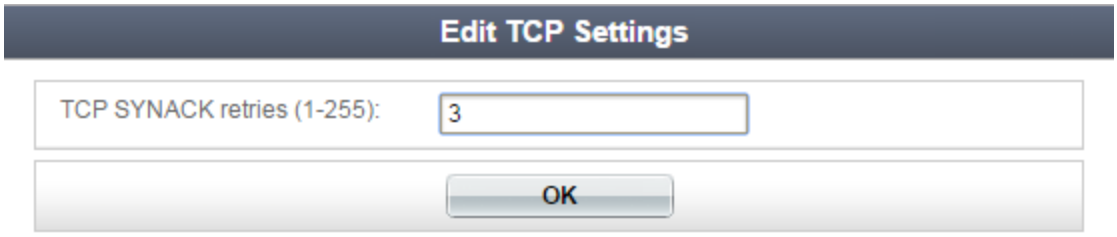
Enter the username and password then select *OK* to test the RADIUS authentication and view the authentication response and returned attributes.

Select *Exit debug mode* to deactivate the debugging mode.

TCP Stack Hardening

As of FortiAuthenticator 4.2, you can now configure the number of TCP SYNACK retries for the Linux kernel by accessing:

`https://<FortiAuthenticator IP Address>/debug/tcp_tuning`



From here, enter the number of retries between 1 - 255 (default is 3).

Filter Syntax

This chapter outlines some basic filter syntax that is used to select users and groups in LDAP User Import, Dynamic LDAP Groups, and Remote User Sync Rules.

Filters are constructed using logical operators:

=	Equal to
~=	Approximately equal to
<=	Lexicographically less than or equal to
>=	Lexicographically greater than or equal to
&	AND
|	OR
!	NOT

Filters can consist of multiple elements, such as `(&(filter1)(filter2))`.

More information about the query syntax of AD filters, see the following web sites:

- http://msdn.microsoft.com/en-us/library/windows/desktop/aa746475(v=vs.85).aspx
- http://social.technet.microsoft.com/wiki/contents/articles/5392.active-directory-ldap-syntax-filters.aspx

Examples

The following examples are for a Windows 2008 AD server with the domain *corp.example.com*, default domain administrators and users, and an additional group called FW_Admins:

- Users (CN) = atano, pjfry, tleela, tbother
- FW_Admins (Security Group) = atano, tbother

An unfiltered browse will return all results from the query, including system and computer accounts. To prevent this and only return user accounts, apply the filter `(objectClass=person)` or `(objectCategory=user)`.

Even if unfiltered, only user accounts will be imported, so this is only required to clean up the results that are displayed in the GUI.

To filter and return only members of the security group: `(&(objectCategory=user)(memberOf=CN=FW_Admin,DC=corp,DC=example,DC=com))`.

It is not possible to use the filter to limit results to CNs or OUs. To achieve this, you must change the Base DN in the LDAP Server configuration. For example, to return only users from the CompanyA OU, create an LDAP Server entry with the following Base DN: `OU=CompanyA,DC=corp,DC=example,DC=com`.

Caveats

Users do not always have a *memberOf* property for their primary group, this means that querying system groups, such as Domain Users, may return zero results. This can be confusing as these are often the first queries to be tried, and can lead the user to think the filter syntax is incorrect.

For example: `(memberOf=CN=Domain Users,CN=Domain Admins,DC=corp,DC=example,DC=com)` will return no valid results.

To return all users in such a group, the filter can be made against the ID value of the Primary Group. So, for Domain Users (Group ID = 513), the filter would be: `(primaryGroupId=513)`.